IPVideoMarket.info

Security Manager's Guide to Video Surveillance

Version 2.2 / January 2009
John Honovich
IPVideoMarket.Info

Contents

I. Introduction/Tutorials on Video Surveillance

Chapter 1: How to Design Video Surveillance Solutions....8
Chapter 2: Introduction to NVRs / IP Video Software....19
Chapter 3: Introduction to Video CODECs....24
Chapter 4: Bandwidth Basics for Video Surveillance....29
Chapter 5: Examining Video Analytics....34
Chapter 6: License Plate Recognition Tutorial....38
Chapter 7: Introduction to DVR/NVR Storage Optimization....42
Chapter 8: Wireless Video Surveillance Tutorial....48
Chapter 9: API and System Integration Tutorial....53
Chapter 10: How to Integrate Video With Other Systems....57
Chapter 11: How to Migrate from Analog to IP Cameras....60
Chapter 12: Directory of On-Line Video Surveillance Tutorials....65

II. Evaluating Key Trends and Technologies

Chapter 13: IT Is Not Taking Over Security....71
Chapter 14: Will Security Integrators Survive?....74
Chapter 15: Should I Use IP Cameras?....79
Chapter 16: Top 5 Problems of IP Cameras....84
Chapter 17: Value of Hybrid DVRs/NVRs....87
Chapter 18: New Options for DVR/NVR Storage....90
Chapter 19: The Value of Centralized Video Analytics....97
Chapter 20: Examining 'Open' Systems....99
Chapter 21: The Danger of Buying Packages....102
Chapter 22: Introduction to City-Wide Surveillance....104
Chapter 23: Is Public CCTV Effective?....108

III. Evaluating New Products

Chapter 24: How to Read Marketing Material....118
Chapter 25: How to Evaluate New Technology....121

Chapter 26: How to Calculate Video Surveillance ROIs..128

About IP Video Market Info

Personalized News

Want to stay informed of new trends, analysis and technology for video surveillance? IP Video Market Info offers the most extensive daily and deep coverage in the industry. Stop by the site or sign up for personalized news.

2009 Industry Guide

If you want more in-depth competitive and industry analysis, consider our 2009 Video Surveillance Industry Guide. This Guide provides recommendations on how to plan and respond to the recession, evaluating what technologies, products and companies will do the best in 2009. The 247 page guide can be downloaded and printed out for easy reading. A premium product, the cost is as low as $40.00 USD for personal use and $200.00 USD to share with anyone in your company.

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?

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.

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 farer 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 product 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 increasingly 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 though 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: Introduction to Video CODECs

Video surveillance systems do not use uncompressed, 'raw' video because of the huge storage that uncompressed video demands. Video is always compressed so that storage and bandwidth costs can be minimized.

CODECs are a critical element of choosing, designing and using video surveillance systems. CODECs can lower the price of overall systems and increase the usability of systems. As such, having a basic understanding of what a CODEC is and why CODECs are used is important.

Fundamental Principle of CODECs

The most important factor to understand in video CODECs is that CODECs help balance off different costs.

For instance, let's say you want to go to the mall and to the supermarket. A few years ago, when gas was cheaper, you might have done this in 2 separate trips. Now that gas prices have increased dramatically, you might want to combine those trips. What's happening here is that as gas has become more expensive, you are willing to trade off lower convenience for savings in cash.

Likewise, using CODECs is a balance between the cost of storage, bandwidth and CPUs. Specifically:

> *CODECs reduce the amount of bandwidth and storage needed at the expense of using more CPU cycles.*

As such, selecting a CODEC always requires you to understand the trade offs in cost between using less bandwidth and storage or using less CPU cycles.

Generally CPU cycles are cheaper than bandwidth and storage so more advance CODECs save you money. Sometimes, CODECs can be too demanding, especially with megapixel cameras and can potentially cost you more in CPU than you save in bandwidth and storage.

Please read my basic bandwidth tutorial for a review of bandwidth's impact on video surveillance.

CODECs Overview

Video must be digitized for it to be used and viewed on a computer. CODECs are means or choices in how we make the video digital.

CODECs or compression / decompression technologies are used to modify the video that is being digitized. Similar to how you might ZIP files on your PC, the video is compressed on its way into the computer. And just like with opening a ZIP file, the video is decompressed before you use or view the video. Unlike ZIP files, the compression of video loses some of the information (engineers refer to this as lossy compression). However, with the appropriate settings, a user cannot tell the difference visually.

Just like in the movies or TV, video is a series of images that are displayed rapidly one after the other. In the US, TV consists of displaying a series of 30 images per second. When we view these 30 images per second, it's “video” and it looks smooth. The fact that video is made up of a stream of images is quite important for understanding CODECs.

When you use a CODEC, you can compress the video in two fundamental ways:

- Compress the individual image by itself

- Compress a series of images together

When you compress an individual image by itself, you simply take the image, run the compression and output the saved file (technically called intraframe compression). Just like when you use Microsoft Paint and save as a JPEG, video compression of individual images works quite similarly. The difference with video is that you need to do these for a continuous stream of images. As such, rather than simply being a JPEG, it is called Motion JPEG or MJPEG.

The benefit of MJPEG is that it requires very low CPU use. The downside is that storage and bandwidth use can be quite high.

When you only compress an individual image, you ignore what's going on between multiple images in a sequence and often send redundant information. If you are streaming video at multiple frames per second, you often are sending basically the same image over and over again. This can be quite wasteful. It's similar to someone calling you up every minute to tell you nothing changed. It would be far better for the person to only call you when news occurred. You can simply assume during the rest of the time that the status is the same.

When people talk about the benefits of MPEG-4 and H.264, not sending repetitive information is the core source of their strength. Every so often these CODECs will send a whole image. The rest of the times they only send updates describing what parts of the image have changed (technically called interframe compression). Since it is common that large parts of the image remains the same, this can result in very significant reductions in storage and bandwidth. For example, where MJPEG may send image after image at 100 KB, codecs like MPEG-4 or H.264 may send the first image at 100 KB but the next 3 or 4 images at only 10 KB each. This approach can reduce bandwidth and storage use by 50 – 90%.

The downside with this approach is that it takes more work for the computer to do this. When you are simply compressing individual images, you do not need to worry about what happened before or what the next image will contain. You simply apply the compression rule and execute. With MPEG-4 or H.264 you need to examine groups of images and make complex calculations of what changed and what did not. You can imagine this can become very complicated and consume lots of CPU resources.

H.264 and MPEG-4 are similar in that they both reduce bandwidth and storage by examining groups of images when they compress video. A key difference with H.264 is that it uses much more complex and sophisticated rules to do the compression. Because H.264's rules are more sophisticated, they can reduce bandwidth and storage even more than MPEG-4. However, the trade-off is that it takes more CPU cycles to do it.

Looking at Current Video Surveillance Systems

The general trend in video surveillance has been a continuous movement to CODECs that save bandwidth and storage. Historically, you have seen products move from MJPEG to MPEG-4 to H.264. The reason why this has happened is because the cost of CPUs to compress the video has decreased faster than the cost of bandwidth and storage. Most experts expect this trend to continue.

Recently, the biggest challenge using CODECs in video surveillance systems has occurred with the rise in megapixel cameras. For years, the maximum resolution of security cameras was constant. All of a sudden with megapixel cameras, the resolution of security cameras has increased by 400% to 5000% or more. The greater the resolution, the harder the CPU needs to work and the more cycles that need to be allocated.

The huge increase in resolution is a little similar to the jump in gas prices. It has changed the economics of CODECs. Whereas historically, for standard definition security cameras, CPU cycles were cheaper than bandwidth and storage. Now, since so much more CPU cycles are needed, it can cost way more in CPU than what you save in bandwidth and storage. As such, almost all commercial megapixel cameras use MJPEG.

One of the most important elements in the next few years will be the development of new approaches and use of new CPUs to reduce the cost of using H.264 for megapixel cameras. Much like alternative energy development hopes to bring the cost of energy down, new approaches are being sought to reduce the use of CPU cycles in compressing megapixel camera feeds.

Conclusion

Understanding the basic choices in CODECs and rationale for choosing CODECs is a key element in video surveillance systems.

Security mangers should consider:

- The video quality of a manufacturer's video (this can vary widely depending on the codecs, the settings and the implementation).
- Generally favor the use of a more powerful CODEC as it can save hundreds of dollars per camera in reduced storage costs.

Chapter 4: 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:

	Bandwidth Generally Available
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':

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

	Bandwidth Cost
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 5: 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 6: License Plate Recognition Tutorial

License Plate Recognition is perhaps the most mature and ready to use video analytic available for security managers today.

Nevertheless, LPR is a very demanding application that can only succeed in limited operational conditions deployed by expert security integrators.

Historically, publicly available information clearly explaining the operational impact has been hard to find. Thankfully, Milestone has released their LPR administrator's manual providing an honest, clear and concise explanation. I recommend you read pages 29-35 to get a very rapid but deep review of the key factors. Though this is for Milestone the points are generally consistent with the state of the art in currently available commercial systems.

The Milestone document helps to reveal 3 key practical elements:

1. LPR can only succeed when a number of strict operational conditions are met.
2. The costs of achieving these conditions makes LPR unfeasible for many scenarios.
3. You need deep security integration expertise to succeed but only modest IT depth.

The Conditions

Here are the key conditions that need to be meet in approximate order of difficulty:

1. US license plates need to be at least 130 pixels wide. This translates roughly into an image no wider than 5-6 feet assuming standard definition video (640 x 480 pixels or 4CIF). That's a very tight shot.

2. The horizontal angle between the camera and plate is within 20 degrees. This means that if your camera is 10 feet away from the plate, the plate cannot be more than 3 feet to the right or left of the camera. This significantly limits where you can put the camera.

3. The vertical angle between the camera and plate is within 30 degrees. This means that if your camera is 10 feet away from the plate and the plate is 3 feet off the ground, the camera cannot be mounted more than 8 feet high. This usually can be accommodated but is low relative to normal heights for outdoor surveillance.

4. There are a host of lighting adjustments that need to be made. Simply using a stock camera with stock settings will routinely cause very poor performance. For example, Milestone recommends CMOS cameras, disabling auto gain, using WDR and higher shutter speeds (if the car is moving). There are many advanced details that need to be set correctly.

Almost all successful LPR deployments used specialized cameras, often manufactured specifically for license plate rate recognitions. These cameras generally have built-in infrared illuminators and pre-set configuration optimized for filtering out lighting issues.

5. You must use MJPEG and you cannot use H.264 or MPEG-4. Since the analytics in this design are being done outside of the camera and since the analytic can only process images, MJPEG is required. You could theoretically use H.264 or MPEG-4 but then you would have to decode it and the processing power can be very significant. Bottom line is this can have a big impact on bandwidth utilization especially if you are looking for a wireless system.

Feasibility

Clearly, LPR is feasible for the traditional license plate camera use case: A camera installed immediately adjacent to an entrance or toll booth that is only a few feet off the ground and dedicated to looking at the plate. Automated LPR makes reading these plates easier.

However, for broader market usage, this has major limitations. Lots of companies like the concept of monitoring the license plates of people who enter their premises. Setting up cameras in the specific constraints required can be very expensive. Assuming you can find a location that meets these constraints, it requires a construction project that can be $5,000 or more per camera simply for the installation and equipment.

The holy grail is reusing your PTZs mounted on roofs and poles. However, these conditions should make it clear that is not feasible. One, getting the resolution needed would be difficult. Does a monitor manually zoom in on license plates? Even if he does, what will the image quality be, given the lighting constraints required for LPR. Also, it will be extremely tough to stay within both the horizontal and vertical angle requirements.

LPR analysis, with its current capabilities, cannot enable significantly new operational uses of license plate monitoring. While it should help with the traditional use case of monitoring controlled traffic flow, its constraints make it very challenging for broader use.

Security Integration Expertise

The other interesting element that the Milestone manual demonstrates is that LPR integration does not demand deep IT skill but it does demand deep expertise in security design and camera systems.

Integrating LPR is much more like using a graphics design application than it is like setting up a mail server. It depends on understanding the design objectives of security, the physical conditions of the site and the capabilities of the video tools available. The IT elements of the setup are fairly straightforward for a security integrator. The challenge lies in the design and application.

Chapter 7: Introduction to NVR/DVR Storage Optimization

Storage optimization is a major concern for security managers as storage costs for video surveillance have always been a large portion of the overall purchase price.

Megapixel cameras have brought renewed interest in measures to maximize NVR/DVR storage duration and use. Cost is a big factor as the potential storage needed could increase by 10x or more than historical standards. Understanding what options and measures are available is becoming increasingly important to selecting NVRs/DVRs and designing IP video systems. This report surveys common measures used to maximize storage duration and use.

Recently, interest has risen in new product categories that specialize in optimizing storage use. Frost and Sullivan has recently reviewed "Video Lifecycle Management Solutions" and identified TimeSight Systems as a "young leader" in this space. The release does a good job of identifying the problem and highlighting one potential solution.

As almost all video systems have numerous measures to optimize storage use, I recommend that integrators and end users focus on utilizing existing measures in leading systems. Video system developers have been building tools for years to address storage optimization. Most will be best served by selecting a video management system based on features optimized for your specific security needs. Significant and comparable storage optimization can generally be accomplished on most mainstream NVR / DVR systems.

How Do I Optimize Storage?

This report reviews 8 commonly available storage optimization functions available on mainstream NVR /DVR systems. Though not every system has all of these features, all systems offer a number of them, providing strong storage optimization.

Here is the list:

- Basic Motion Analytics
- Advanced Video Analytics
- Motion Exclusion Zones
- Data Aging
- Recording Schedule
- CODEC Selection
- Dual Streaming
- Storage Clusters

Advanced Video Analytics

Now that video analytics are getting accurate at detecting people, faces and vehicles, this intelligence can be used to control recording. I believe this will become one of the most powerful new areas of storage optimization in the next 3 years. Long term storage can be optimized by selectively recording objects most likely to be of long term interest - people, faces and vehicles. Traditionally, long term storage optimization techniques reduce the quality or the frame rate of all video uniformly. With video analytics, storage optimization techniques can become smarter, increasing the probability of possessing quality long term evidence while minimizing total storage consumed.

For instance, in addition to recording video, 3VR records all faces seen on cameras. Faces of all the people (100,000+) conducting transactions at a bank branch can be stored at 4CIF quality with less than 20GB of storage. This is 1/100th the amount of storage needed for video and the most important evidence for retail bank's security needs. Of course, today this is just faces but the same process can and will certainly eventually be used to store all the people seen, all the cars moving through an area, etc.

Video analytic companies specializing in perimeter violation are reducing storage needs for those cameras by 90% or more. By placing intelligence in the camera, the camera can only stream or the management system can only record specific objects of interest. For cameras whose main purpose is real time alerting, this is a great storage win. Of course, many cameras are needed for investigation purposes and need storage. As such, this is simply another tool in our collection.

Basic Motion Analytics

Most video surveillance deployments use basic motion analytics to control recording. Because most facilities have significant periods of low activity (e.g., nights, weekends) and areas of low activity (e.g., hallways, stairwells), motion analytics can reduce storage consumption by 50% to 80%. Most systems set their basic motion analytics to be fairly conservative so that they rarely miss real incidents. As such, basic motion analytics is trusted and used by many military bases, banks and Fortune 100 companies and most real world deployments. Of course, some facilities do not want to take any risk and require continuous recording.

A nice balance that is sometimes achieved is a combination of continuous and motion based recording with a baseline level of continuous recording (e.g., 3 frames per second) and motion based recording set higher (say to 15 fps). This ensures that video is always recorded but storage use is optimized for when activity of interest is most likely to occur (that is, when motion is detected).

Motion Exclusion Zones

Using basic motion analytics to control recording is enhanced through using motion exclusion zones. It is common for cameras to cover areas that are not of interest to users. Examples include highways behind the building, a tree out front, windows, ceiling lights, etc. Taking a few minutes to set up motion exclusion zones can reduce the storage utilization by up to 50% on certain cameras. After the first week of a new install, a review should be conducted to tune these settings.

Data Aging

Many systems reduce the number of frames in stored video as the video is older. The basic premise is the older the video, the lower the probability that the video is relevant. Rather than simply delete the video, the size of the video is reduced so that some evidence is available just in case but the storage costs are minimized.

For instance, March Networks has a feature called "Intelligent Video Retention." Avigilon has an advanced data aging solution that specializes in optimizing storage for multi-megapixel cameras. In higher end video systems, this type of feature is frequently available. It's quite useful because it can easily double storage duration.

Recording on a Schedule

Many organizations have greater security risks at different times of the day. Schedules are a common feature to adjust recording parameters to match those different level of risks. For instance, an organization may want continuous recording during business hours but is OK with only having motion based recording after hours. Making this adjustment can reduce video storage use by up to 40%.

CODEC Choice

Choosing a video CODEC that provides the most efficient storage utilization has been a key component of video system designs for years. While technical issues exists, the trend of moving from less efficient to more efficient CODECs is clear (e.g., from MJPEG to MPEG-4 to H.264). The key practical issue currently is the use of H.264 for megapixel cameras due to the high system requirements H.264 demands. With multiple megapixel manufacturers releasing H.264 megapixel cameras, in the next few years H.264 megapixel cameras looks certain to be a reality (at least for lower resolution MP cameras). Migrating from MJPEG to H.264 can reduce storage use by 50% or more.

Dual Streaming

To maximize CODECs' different strengths and weaknesses, multiple video streams can be used. For instance, H.264 may be the best choice for storage optimization but MJPEG has advantages of live monitoring (e.g., lower delay, lower processing power to view). Most cameras support dual streaming. Video surveillance systems can take advantage of this to reduce storage costs while ensuring optimal live video monitoring.

Storage Clusters

Historically, storage was separated into small pools for each unit and options for upgrading storage were limited to a few TBs (at most). Today, with storage clusters for video surveillance maturing, centralized pools of storage can create ~ 30% efficiencies in storage use and make extending storage simple and fairly inexpensive. If you are interested in learning more, read my extensive analysis of storage clusters.

Conclusion

While by no means comprehensive, this survey should help engineers and users to identify and use commonly available measures to optimize storage duration. Understand what your systems offer and make use of those features. By doing so, you will be able to optimize the storage of most any DVR or NVR and accommodate increasing storage demands.

Chapter 8: 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.

Let's review these key elements:

- How much bandwidth is available?
- How far away can the wireless cameras be?
- How many cameras can I deploy?

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 your 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 constrains, 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 9: 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 pre-requisite 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 10: 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.

Chapter 11: How to Migrate from Analog to IP Cameras

Migrating from analog to IP can be tricky, mainly because most everyone has existing infrastructure in place. You rarely can simply throw out that infrastructure and start anew - the economics usually do not support it. Because of that, you need to figure out what to keep, what to replace and what to modify.

The issues involved are too complex to provide a simple boilerplate yes or no. This report examines the most critical elements in making the transition from analog cameras to IP cameras so that you can better appreciate the issues involved for your circumstances. Nonetheless, you will have to spend significant time learning and evaluating as the issues involved are significant.

Here is a summary of those key elements:

- Determine if your DVR supports IP cameras
- Determine what IP camera manufacturers your DVR support
- If needed, assess options for NVRs or IP Video Management Software
- Determine if IP cameras can eliminate long distance analog cabling
- Determine if higher resolution cameras can help you
- Assess the increased bandwidth impact on your networks
- Determine if you can afford increased storage for megapixel cameras

DVR Supports IP Cameras

First check whether your DVR supports IP cameras. Most DVRs that cost more than $3,000 USD usually supports some form of IP cameras today. However, most of the more 'budget' type DVRs do not.

You should determine this first because it is the key element in determining how complex adding in IP cameras will be. If your DVR does not support IP cameras, you have a few options, none of which I think are very attractive: (1) you could monitor the IP cameras directly with no recorder, (2) you could set up a separate NVR to record the IP cameras or (3) you could decode the IP camera's video stream to record them on your existing DVRs. Most professional security organizations want a single video management system to record and access all cameras which means that you either work with what you have or replace it.

Which IP Cameras Your DVR Supports

If you DVR supports IP cameras, you definitely need to find out which manufacturers and models of IP cameras they support. Many DVR suppliers only support 1 or a small number of IP camera manufacturers.

This can be really confusing and surprising coming from the analog camera world. With analog cameras, no one worried about whether a DVR could support a fixed camera because once you supported 1 analog camera, you supported them all. However, with IP cameras, you have to check every time for not only manufacturer support but for specific model support (i.e., a DVR manufacturer may support the Axis 207 but not the Axis 221).

Determining what IP cameras a DVR supports is very important because different manufacturers specialize in different types of products. If your DVR only supports 1 or 2 camera manufacturers, this could cause significant problems. For instance, there are specialists in high end, standard definition cameras (Axis); budget standard definition cameras (ACTi); inexpensive multi-megapixel cameras (Arecont Vision); high end multi-megapixel cameras (IQinVision), etc. You need to determine what types of IP cameras you need and whether those are supported by your DVR.

These first two points will help you understand the degree of difficulty of adding in IP cameras.

NVRs or IP Video Management Software

At this stage many will reach a point where you need to consider replacing your

DVR system. The emerging alternative are designed to support dozens of IP cameras. If you get to this point, this will be a challenge in and of itself. There are dozens of companies that offer NVRs or IP Video Management software.

Furthermore, if you head in this direction you will need to determine how to support your existing analog cameras. Because IP Video Management Software only supports IP video streams, you will need to purchase encoders to convert the analog video stream from your camera into an IP video stream that the IP Video Management software can handle. Encoders are fairly expensive ($300 - $600 USD per camera) so it may be worthwhile but it is not without its costs.

This covers the fundamental product options and choices. To determine if the migration is worth it, focus on the next two items.

Eliminate Long Distance Analog Cabling

All cameras need to be connected to a video recorder. How they are connected can vary greatly. The most common means for analog cameras is to use a dedicated coaxial cable to connect the camera to the DVR. Indoors and over short distances, this is usually quite simple to do. However, if you need to go long distances, outdoors or through areas where it is hard to run a new dedicated cable, analog cameras can become problematic.

If you have multiple buildings or outdoor areas to protect, you may not be currently using surveillance cameras or if you are you had to resort to expensive proprietary transmission systems. This is the most valuable and powerful use of IP cameras. With IP cameras, you have the potential of reusing existing networks in your facilities. You also can use low cost IP wireless equipment to add cameras in distant or outdoor locations.

To the extent that this situation applies to you, your motivation to move to IP cameras should be stronger. It can either reduce costs by thousands of dollars compared to existing implementation or enable you to add new cameras in places that would have been previously cost prohibitive.

Use of Higher Resolution Images

IP cameras offer the potential to capture and record much higher resolution images than analog cameras. While the maximum resolution of most IP cameras is the same as most analog cameras, one type of IP camera, the megapixel camera, can offer far greater resolution.

You should determine how and where you can make most use out of megapixel cameras. Key determinants are (1) the greater the area you want to cover and (2)the higher your need to see details. For example, a parking lot or cashier's station. By contrast, if you are observing a small office room and just need to know when someone was inside, a traditional standard definition analog camera will do fine.

Megapixel cameras come with two huge impacts that you must consider when migrating from analog cameras: bandwidth and storage.

Assess the Bandwidth Impact

When migrating from analog to IP, if you keep the resolution you record at the same, the impact on bandwidth (your computer network) should be minimal. For instance, most commercial users record at 5 frames per second at CIF (320 x 240 pixels). At these levels, bandwidth consumption is quite low (under .5 Mb/s) relative to today's networks (100 Mb/s ++). Even with a few dozen cameras, this should not make a significant impact on even lower end switches.

However, if you want high resolution or frame rates, then you need to start carefully assessing the impact. With these conditions, each camera can consume 5Mb/s to 45 Mb/s, which starts adding up. While you can purchases networking equipment that can handle 1000Mb/s or more, you should not assume that this is already in place and that you can just plug this in.

You certainly should test the bandwidth load before deployment. You may need to consider one of the following two options:

1. Use a separate IP network for the cameras.
2. Upgrade your existing networking equipment to make sure that it can support the load.

Both are certainly expensive and can have a significant operational and political impact with your IT's organization. Though this can be accomplished, do not take it for granted as the cost and complexity can be significant.

Assess the Storage Impact

In a similar manner, increasing the video quality, certainly impacts storage needs. If you use DVRs, you are likely used to buying storage bundled with the DVR (e.g., a DVR with 250 GB or 500GBs of storage for 16 cameras). With IP cameras and, especially with megapixel, you can easily be looking at 1TB per camera, which is a very significant increase. This could increase the cost of your system by tens of thousands of dollars.

You will need to better determine how significant this will be and your willingness to spend more for storage. Some organizations will find it to be no big deal but others may be shocked.

Conclusion

Hopefully this helps identifies key points so you can better assess your situation.

Please ask questions, add other points and debate the appropriateness of the recommendations made.

Chapter 12: Directory of On-Line Video Surveillance Tutorials

Basic Lighting for Cameras from axis
Description: "Lighting is a key element in providing high quality images. Lighting is commonly measured in lux. Measuring lux is not easy for most people. This resource from Axis provides a slideshow of example images with lux ratings. If you know what lux is, this will give you a better appreciation of how to guess / measure how much lux in any scene."

Basic Overview of Security Cameras from electronichouse
Description: "If you are not familiar with security cameras at all, this article will provide a nice introduction. Though the article is focused at the home surveillance market, the information provided is generally applicable to all segments of video surveillance."

Introduction to Lenses from cctvfocus
Description: "Lenses are a critical but often overlooked component of video surveillance. In this tutorial by Vlado Damjanovski, the author of the 'CCTV Bible', Vlado explains the fundamentals elements of lens design and selection. You should have a moderate understanding of cameras to get the most out of this tutorial."

IP Cameras
How to Set up An IP Camera from axis
Description: "This is a very nice video from Axis on how to set up/configure an IP camera. As long as you know the basics of IP cameras, this tutorial should be very

useful. It provides a very clear sense of simple and powerful configurations that can be done to optimize the use of IP cameras."

An Introduction to H.264 from securityinfowatch
Description: "A very comprehensive introduction to H.264 that covers both the benefits and the technology details of H.264. As this is a quite technical article, you should be comfortable understanding other CODECs such as MJPEG and MPEG-4 before reading this article."

What is an IP Camera? from axis
Description: "For the very basics in what an IP cameras is, start with this tutorial from Axis. From this tutorial, you can watch a video on IP cameras or explore details on further pages inside. This tutorial does not require technical expertise and is good for all audiences."

Introduction to Power over Ethernet for IP Cameras from sdmmag
Description: "Using Power over Ethernet with IP cameras is a major change from traditional analog camera deployment. It offers significant reduction in complexity and cost. Nevertheless, it is a new technology to many in video surveillance/physical security. this tutorial does a nice job of explaining the issues involved. Moderate understanding of computers and networks will be helpful for this one."

Megapixel Cameras

Introduction to Megapixel Cameras from securityinfowatch
Description: "This tutorial provides an introduction to the use and benefits of megapixel cameras. While a basic background in video surveillance is helpful, you do not need to know much about megapixel cameras to learn from this piece."

NVRs/IP Video Software

Introduction to Video Encoders from sdmmag
Description: "Encoders are an important component of network-based video management and recording. Encoders allow analog cameras to work with NVRs. This article is an excellent overview of what encoders are and what role they play in video surveillance systems. It does not require special technical expertise."

Video Analytics

Webinar Introduction to Video Analytics from isc365
Description: "This tutorial is a webinar where you can watch and listen as examples of various video analytics are demonstrated. This is good for the beginner as it does not require any specific technical expertise or background."

How to Position Cameras for Perimeter Violation from ioimage
Description: "One of the most fundamental but underappreciated components of using video analytics is setting up cameras. This tutorial, from ioimage, does a good job of honestly examining the many details important to making perimeter violation work in the field. Even if you do not know much about camera functionalities, viewing the tutorial should give you a feel of the steps needed."

How to Test Perimeter Violation Analytics from ioimage
Description: "Marketing videos often leave the impression that a video analytics system works if it can simply alert when a person is casually walking through the scene during the middle of the day. This tutorial, from ioimage, demonstrates the many different scenarios that a production video analytic should be able to handle. You may not actually ever do this test but reading this tutorial should give you a better appreciation for the real measures an adversary may attempt to beat your

system. This tutorial does not require any technical expertise."

Networking

Designing IP Networks for Video Surveillance from isc365
Description: "This is a mid-level to advanced tutorial that explains the key points and design elements in designing IP networks for Video Surveillance. This tutorial is a 1 hour webinar hosted by Cisco Systems. The first part will be valuable for a general audience as it reviews the basics of networking. The second part on QoS techniques really requires a background in networking to be useful."

Introduction to IP Multicasting from indigovision
Description: "Multicasting can provide significant bandwidth reduction when many users want to view the same live stream. However, multicasting is not simple. This tutorial, from IndigoVision, provides a nice overview of the benefits, challenges and steps needed in deciding and using multicast. The tutorial assumes a moderate level of IT/networking concepts."

Technical Basics of IP Networks from axis
Description: "If you are not comfortable with basic technical terms and concepts of IP networks but want to learn them, this is the right tutorial for you. It is a gentle overview of the basic elements important to you in dealing with IP networks for video surveillance."

Convergence

An Introduction to PSIM from securitydreamer

Description: "PSIM, or Physical Security Information Management, is an important emerging force within security and video surveillance. With camera counts continuing to grow and video analytics generating information, the demand for an organized and systematic way to manage this information."

II

Examining Key Trends and Technologies

Chapter 13: IT Is Not Taking Over Security

So much talk today focuses on the power of IT and what IT is doing to security. While security managers will certainly leverage that technology, IT is not replacing or taking over security.

Automation is a powerful economic force, one that will ultimately make IT irrelevant to physical security. It may seem paradoxical but the same force that makes information technology ubiquitous will make IT irrelevant to physical security.

Physical security will certainly use more technology than ever before but the technology will become easier to use and deploy. As it becomes easier to use and deploy, the need for IT decision making and IT personnel will diminish and become a minor factor. Companies like Io Image are already showing us this future while big IT companies such as Cisco and IBM are stuck in the past. In the security industry, it's easy to fear that we are being gobbled up by IT but it's just a phase.

The ROI of Automation and Simplicity

This is easy to predict because the economics demand this and the history of other fields demonstrate this.

IT has been assimilated into every department in the enterprise and after the initial introduction, control always returned to the department. The first financial systems and CRM systems were huge complex projects that demanded custom software development and extensive on-site administration. IT obviously had to be heavily involved. Today, the sales manager can get up and running for little money and hassle from Salesforce.com, etc. The sales manager has a huge incentive to simplify because he does not want his sales operations hindered by never-ending IT projects. He will engage IT for support and services but he uses their input to make his own final decision. The same will happen for security.

Whenever technology is complex and unpredictable it requires extensive analysis, planning and field integration/ support. This is a characteristic of early stage technology. The first DVRs had this characteristic. The first IP cameras, megapixel cameras, analytics, etc did as well. 10 years ago DVRs were a major IT project and now they are ubiquitous, can be purchased at Costco and installed by the store manager. Technology vendors saw that their sales were limited due to the extensive on-site integration, testing and planning needed. To increase their own sales, they worked hard to simplify and eliminate deployment challenges. As this happened, IT became less and less important and the DVR needed only rubber stamp approval from most IT departments. The decision making returned to the security manager who now only focused on which product best helped him meet his security goals.

Cisco and IBM do not get IT

In perhaps the greatest irony in our industry, the two biggest 'IT' companies just do not get it. They bring to market incredibly complex, expensive systems that demand extensive field integration. From Cisco and IBM's perspective, maybe this looks like great business because the products are expensive and the follow-on services are substantial. But from the customer's perspective, this is awful. This is simply a tax on the customer, dropping the ROI and making the business case more difficult.

With Cisco and IBM, you have to initiate a huge project, get the CIO involved, spend months planning and deploy a team of engineers/consultants.

Io Image is showing us the future of advanced IT technologies in the physical security space. Let's contrast what Io Image is doing to what Cisco and IBM have done.

ioimage **does get IT**

ioimage's slogan is "Designed for Simplicity" and you can see from their product design to their distribution strategy, that making it simple to purchase, setup and deploy is a key business objective.

Do you know where you can buy Io Image products from? Northern video and now, SuperCircuits. That's right, SuperCircuits -- The magazine you get with the $12.95 pinhole spy cameras now offers Io Image video analytic cameras. This is a great thing for security buyers but a signal of the problems for Cisco and IBM.

While Cisco and IBM are making it expensive and complex to use advanced technologies in physical security, Io Image is making it easy. Io Image is making it so easy that it's reducing the need for IT to be involved. Io Image let's the security manager concentrate on meeting his security goals. So while Cisco and IBM may be friends with the CIO, companies like Io Image will enable the highest ROI by delivering affordable and easy to deploy technologies.

ioimage's strategy shows the future of physical security. It's a future of ubiquitous technology freed from the cost and complexity of big IT.

Though technology has been and will continue to be a key force in physical security, IT's importance is just a phase. IT does not get this but Security Managers and Integrators should have faith in this.

Chapter 14: Will Security Integrators Survive?

Almost all security managers use security integrators. As such the fate of security integrators and the value of continuing to use security integrators is a key question today.

Many believe security integrators are dead; walking dinosaurs who are oblivious to their impending extinction. Indeed, many new IT entrants certainly wish that security integrators (and physical security managers) are wiped out.

Despite this belief and hope, is this really the case? **Are security integrators destined to fail?**

No, **I believe security integrators, as a whole, will survive**. I believe the detractors have made 3 main mistakes:

- Detractors look at convergence as a recent phenomenon whereas security integrators have been adapting for the last 10 years
- Detractors do not appreciate the skills that security integrators possess
- Detractors view IT as a disruptive innovation when it is truly a sustaining one

Adapting for 10 Years

Security integrators have been assimilating IT skills for the last 10 years. While a lot of anxiety exists over IP cameras and NVRs, the technical challenges were far worse 8 to 15 years ago. At that point, integrators were deploying their first DVRs or network based Access Control systems. Most had no IT skills. Many did not even know what an IP address is. Over the years, with education and on the job experience, the situation has changed dramatically. Today, most security technicians have at least basic IT skills and many are fairly sophisticated. IP cameras and NVRs present new technical challenges but they are extensions of the basic skills security technicians have been learning for years.

I am not contending that security technicians are as strong in IT as IT technicians. However, there are 4 very real aspects that affect the competitiveness between IT and security integrators:

- IT technicians are much more expensive than security technicians
- Security technicians have a good basis for the tasks needed for IP security systems
- As IP based security systems mature, they are becoming easier for non-IT experts to use
- A lot of what IT technicians know is overkill for IP security systems

Because they have been adapting for the past 10 years, security integrators can offer many of the IT skills needed at less cost than IT integrators. This is an under-appreciated factor in why security integrators will survive.

Security Integrators' Skills

Many underestimate the importance of security integrators' skills and the value those skills will continue to have in projects. Two key issues exist:

- Security Integrators have many key skills that IT Integrators lack
- Even in IP security systems, most of the integration work is not IT

Good security systems integration requires extensive design and implementation precision. It is far more more involved than simply installation plus IT tasks.

Security integrators have been learning skills for years that IT integrators totally lack.

Good integrators in any field participate in design. Just for video surveillance, security systems integrators must be able to:

- Anticipate what areas and assets require protection (many end users need guidance here)
- Determine how to protect those assets with what cameras and what positioning
- Understand the limitations of the products available for protecting/imaging
- Understand the environmental limitations and how to accommodate them
- Determine and eliminate gaps in coverage

None of these are IT tasks but all of these are essential in integrating a high quality video surveillance system.

These skills are needed throughout the implementation and are not a distinct part of abstract design. Rarely can security equipment simply be installed. It requires skill and judgment in how to adapt to on-site issues:

- Judgment and skill in final camera positioning is critical in ensuring the right shot
- Camera settings and lenses will need to be adjusted to optimize image quality
- Cameras may need to be moved due to an unforeseen implementation issue
- On site managers may object to aesthetics and integrator will need to find new positioning

Again, none of these are IT tasks and none of these go away with IP based systems. You need to master these aspects for good security integration. The average security integrator has this. The average IT integrator does not.

The same pattern exists in developing policies and best practices for using security systems. Security Directors routinely expect and lean on their integrators to help teach them and share ideas on how to best use the technology for security objectives. IT skills are of little help here unless you know the application and the issues involved in physical security.

80% of the work involved in security systems integration is in the areas I have just outlined. The IT side is certainly valuable but as a matter of time and effort, it is a rather small portion of overall IT projects. As such, it is a natural candidate for security integrators to simply expand and integrate into their services. And as I have discussed above, this is is part of a long-term trend that security integrators have been doing for years.

IT is a Sustaining Force to Security Integrators

The emphasis on IT being a 'disruptive' technology to security is misleading. Many think disruption is a factor of how sophisticated or powerful a technology is. In a business context, that does not make a technology disruptive. Technologies only disrupt businesses when they disrupt business models. The widely held theory of innovation contends that if a new technology enables incumbents to make more money from their best customers in the same way they have historically, the incumbents usually win.

Security integrators can make more money from their best customers by selling IP based security systems. As such, innovation theory holds that security integrators should survive. Just like they did before, security integrators are still selling products, integration services and maintenance services. Plus, the revenues per deal have generally increased. In the often cited scenarios where incumbents where killed, it was because prices were radically different (e.g., mini-computers vs PCs) or the business model switched from selling products to subscriptions (e.g., SaaS). This is just not the case here. There's no reason to think security integrators will retreat and growing evidence that they are responding.

All the big security integrators are financially motivated to compete and they have resources they can invest in IT. Just like many other industries, security integrators will engage in training and will hire new personnel with appropriate skill sets, assimilating them into their organization. And because security integrators have excellent existing skills in the fundamentals of security systems, they will have a big advantage over IT integrators trying to learn the space, relationships and implementation details that integrators have mastered over the years.

Concluding Thoughts

Running a security integrator, I have lived through all of these elements first hand. At that time, I was the IT outsider brought in to help the transition. However, it was I who assimilated because that made the best business sense. Of course, I brought in new training, practices and skills that helped grow the business. Nevertheless, we used the core group of existing security technicians as the basis, improving their IT skills and supplementing them with a small number of strong IT engineers. It was simultaneously less disruptive, more profitable and allowed us to execute on the many physical security related details that the IT engineers would have taken a long time and a lot of money to sort through.

You may have a couple of counterarguments:

Counterargument: My Security Integrator is Bad

It happens. But consider that about 1/3 to 2/3 of all IT projects fail. Making security into IT is no panacea. IT has plenty of its own issues.

Counterargument: IT is the future - It has to take over Security

To the extent that computers are replacing electronics, absolutely. Security systems will become an IT specialty, just like historically security systems were a specialty of low voltage electronics. However, the companies that succeed in security as an IT specialty are likely to be the traditional security integrators who evolve into this role.

Some Security Integrators have to fail

Certainly, some will fail. Some always fail but the failures will be more an issue of poor individual execution than it is that the whole industry will collapse.

IT integrators have a lot to offer

I agree. Look to see IT engineers hired into existing security systems integrators or see them start their own specialty shops dedicated to security systems. I am only objecting to big IT integrators coming in and wiping out security integrators. There is always room for new skills and new talents to grow an industry.

Chapter 15: 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 16: Top 5 Problems of IP Cameras

The overwhelming majority of people buying cameras today do not choose IP cameras. While most people see the move to be inevitable, serious debate exists on how long it will take to get there. Recently a number of analysts have even slid back projections for when IP camera sales will overtake analog.

To figure out why you should select IP cameras and to figure out when the mass of users will buy IP cameras, we need to honestly and clearly assess what is holding back IP cameras.

The common explanation is a lack of training and a lack of support by traditional integrations and manufacturers. I think these problems are secondary and a consequence of more fundamental problems. Here they are:

Primary Problems

- IP Cameras are too Expensive Compared to Analog Cameras
- Storage for Megapixel cameras is too expensive
- Smart Cameras are still in their infancy

Secondary Problems

- DVRs offer limited support
- Lack of Integrator Training

IP Cameras Too Expensive

It is common knowledge that IP cameras cost more than analog cameras. Compare a Pelco CC3701H-2 to a Axis 211. With the same lenses, the Axis is double the price of the Pelco ($600 to $300). However, this is not the main point I want to make.

To identify the real issues, we need to understand the flaws in Axis well publicized TCO Report on IP vs Analog. The report claims that systems of over 40 IP cameras are cheaper than analog. There is a lot in the report and it is certainly worth reading.

The fundamental problem of the report (and IP camera expense) is that over 90% of customers already have analog systems – DVRs, coaxial cable, analog cameras, etc. The report assumes a greenfield installation with no coax in place and no analog cameras. This is not representative for the overwhelming majority of customers. Once you factor in customers that have analog in place and are looking to upgrade, the costs look far worse for IP camera systems. I would encourage Axis to conduct a follow-up report using this more realistic assumption.

Moreover, being 5% cheaper than an existing technology (which is essentially what the Axis report claims) is rarely sufficient to motivate customers to switch. Indeed, in the applications where IP has been most heavily adopted, it is the elimination of analog video fiber networks that has provided the ROI necessary to migrate to IP cameras.

To make people switch, IP needs to be either significantly cheaper or offer significant economic benefits that analog can not offer. As I reviewed recently, I am encouraged by the ability of ACTi to provide solid, low cost IP cameras that can narrow the cost gap. On the other front, to increase economic benefits, megapixel cameras and video analytics hold the most promise. Let's now examine them.

Megapixel Storage Too Expensive

Compared to analog cameras, megapixel cameras can increase cases solved and reduce camera counts. The biggest economic problem for megapixel cameras is the cost of storage. Almost all megapixel cameras in production today use MJPEG encoding which is 2x to 4x less efficient than the codecs used for analog cameras. Combine this with the massive increase in resolution of megapixel cameras and the cost of storage per camera can be $500 - $1500 per camera up from $50 - $100 for analog cameras.

This is a significant tax that many customers are justifiably concerned. You often hear from vendors that this is not a problem. I believe that for certain high end customers this is true (remembering less than 2% of all cameras are megapixel). However, this will not be the case for mainstream customers. The extra cost for storage will make it very hard to justify mainstream deployments of megapixel cameras.

Yes, H.264 is coming but the questions on how well it will work for megapixel cameras are significant and unanswered.

Smart Camera Infancy

Another way IP cameras can add value is by embedding video analytics into the camera. The challenge here is that smart cameras are not commonly available (even from Axis) and that big questions remain about how well smart cameras will work. Making this even more challenging is that DVR manufacturers are putting analytics directly inside their units. This would extend the life of analog cameras making the case for smart cameras harder.

DVRs Do Not Support

Many DVRs offer limited or no support for IP cameras. This certainly reinforces the problem for IP cameras.

While many IP vendors turn this into a morality play, the lack of support is a reflection of a weak business case. I often hear claims that DVR companies are stupid or greedy. At the heart of it, I believe the real barriers are fundamentally issues of economics – the problems I listed above. Once those problems are resolved, good DVR companies will be be motivated to support and bad ones that refuse will be quickly crushed.

Lack of Integrator Training

I see the same issue for security integrators as for manufacturers. Security integrators correctly see that IP is not ready for most of their customers. As such the motivation is weak. At the same time, security integrators are still doing well and growing. Again, once IP cameras solve their problems, security integrators will be forced to support or will be displaced.

Conclusion

None of the above means that any specific customer should not use IP cameras. Use of IP cameras depends on specific application and logistic uses.

However, I am contending that until the 3 primary problems are solved I do not believe IP cameras will be selected by a majority of customers. The solutions of these problems are:

- Standard Definition IP Camera only costs $100 more than equivalent Analog Cameras
- Megapixel cameras support H.264 and H.264 has no serious side effects on client or servers
- Smart Cameras are widely available and the analytics work reliably

Once these solutions are delivered, the business case will become strong across the board. Integrators and DVR manufacturers will then be forced to support IP cameras or be ousted by rivals that offer the clearly financially preferable IP solution.

Postscript

For an extensive discussion and debate on this topic, read the original report at http://ipvideomarket.info/report/top_5_ip_camera_problems.

Chapter 17: 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 18: New Options for DVR/NVR Storage

For years, storage for video surveillance has been done on board your DVR. You specified the size of the hard drive you need, the manufacturer made sure the right hard drives were installed and your unit was shipped to you. Today, a major new option is emerging that replaces storage in your DVRs/Servers and places them in central clusters of storage.

In the last year, buzz and vendor marketing has grown quickly around clustered storage solutions that could replace the traditional internal storage that has been the standard for many years in video surveillance. Despite early wins being concentrated in a few niche markets (e.g., casinos, municipalities), the fundamentals of these offering indicate they will have a major impact across most of the video surveillance industry in the next 3 years.

This review examines the background, advantages and constraints of storage clusters as a replacement for traditional DVR/NVR storage.

Storage clusters are appliances that are separate from your DVR/NVR and communicate with them across your IP network. Storage clusters are modular and more storage can be added over time, starting from as low as a few TBs to more than 1000 TBs. The most well known specialists offering these solutions are Intransa and Pivot3 .

Recommendation: Use storage clusters when a site has more than ~ 48 analog cameras and/or more than ~ 6 megapixel cameras.

Here is a summary of the key advantages and constraints:

Advantages

1. Price differential between internal storage and storage clusters have dropped dramatically
2. Storage Clusters can reduce storage needs by ~ 30% over internal storage
3. Storage Clusters are actually cheaper for large camera counts and storage durations
4. Storage Clusters are cheaper and better for megapixel cameras
5. Storage Clusters offer RAID 'standard'

Constraints

1. Storage Clusters are not cost-effective for smaller camera counts
2. Storage Clusters cannot centralize storage across most distributed facilities

Advantage 1: Price Differential

Where historically the price differential per unit of storage was huge, today, the differential is small or, in many cases, not at all. This is critical in spurring broader adoption.

Almost all observers recognized that storage clusters were superior to on-board storage but the historical pricing for storage clusters was 300% to 600% more for the clusters. As such, it was incredibly difficult to justify the significant increase in expense and very few video surveillance systems used this solution.

In the past few years, the increasing maturity of these solutions and the utilization of standards based IP networks has shrunk the price differential. The price of the supporting infrastructure to build storage clusters has dropped, enabling the price of storage clusters to fall faster than the price of internal DVR/NVR storage.

Per TB, the price of storage clusters is very competitive with internal DVR/NVR storage. Storage clusters cost about $2,000 per TB. For most mainstream DVRs, the MSRP to add 1 TB of storage is $2500 to $3800. Storage clusters actually can be cheaper than internal storage. I was fairly shocked about this difference but I confirmed with multiple price lists from multiple dealers.

Note: The minimum size storage cluster available today is 4TB which is a big factor in small camera count deployment. This affects total cost for this scenario and will be examined in the constraints section.

Advantage 2: Reduce Storage Needs

When you deploy multiple DVRs, even in the same building and with the same configurations, you often obtain different storage durations. Let's say you target 90 days of storage, some will get 75, others 105, a few 55 and one or two 125 days. This is because storage utilization is a factor of amount of motion or traffic in a camera's view. (PTZs are famous for chewing up storage because of this).

Because storage duration falls in a range, you generally need to deploy more storage than the average system needs or reducing recording settings on systems that do not record as long as you need. In the former, the direct impact is higher installation costs. In the later, the direct impact is higher service costs and the indirect impact can be issues with evidence usability.

With storage clusters, DVRs/NVRs record to a central pool of storage. Let's say you have 10 DVRs and the average DVR consumes 800 GBs of storage to record 90 days. However, because some of the DVRs will need more storage to reach 90 days, you use 1000GB storage in each DVR instead, resulting in a 25% premium. In a storage cluster, because storage is pooled, units that need more storage and balanced off with units that need less. Therefore, you would simply use 8TB of storage and eliminate the 25% padding and premium.

Even in a modest scenario like this you can save a few thousand dollars simply by this pooling effect.

Advantage 3: Cheaper for Large Camera Counts / Extended Storage

Once you get into large camera counts or extended storage, it pushes the limits of what internal storage can provide. As such, the economics of storage clusters are preferable.

Using internal storage will require using the largest hard drives possible (so you can fit in chassis). Larger hard drives are much more expensive (per unit of storage) than smaller hard drives. With a storage cluster, you could use the most cost-effective hard drives sizes and reduce costs.

Using directed attached storage requires an external appliance. Such an appliance will cost a few thousand, even without the drives. At that point, and for roughly the same price, you might as well use a storage cluster that provides far superior scalability.

Advantage 4: Better for Megapixel Cameras

The storage demands of megapixel cameras are severe. You can easily use multiple TBs per megapixel camera because of the increased resolution and the need for MJPEG compression.

Most DVR/NVR appliances are not designed to handle this demand for storage coming from multiple megapixel cameras. You can use direct attached storage but again, for roughly the same price, the added benefits of a storage cluster generally make it the appropriate choice.

Advantage 5: Offers RAID standard

While DVRs have offered RAID for years, the additional cost has been quite high. As such, most users elect not to use RAID. A check of leading appliances indicates going from 1TB non-RAID to RAID increases cost by $1500 to $3000 MSRP. Some systems like 3VR are now offering RAID standard but it's certainly more of an exception than the norm. All in all, though, these premiums are hard to justify.

By contrast, storage clusters offer RAID 'standard'. The incremental cost of using RAID is very low. Plus, these systems are all designed to provide many flavors of RAID right out of the box.

RAID offers two primary benefits for video surveillance systems: (1) save the box from dying and (2) save video from being lost.

Saving the box from dying is the more important of the two. Video surveillance systems that die require emergency service calls and increase the risk that a security incident occurs where no recording nor live monitoring is available.

The economic value of preventing video from being lost is generally low. While the cost of providing RAID continues to be significantly more than no redundancy, only a very small percentage of video actually records incidents that have not been exported. As a practical matter, most security managers have elected to absorb the risk of infrequent losses of incidents rather than pay the significant premium for storage redundancy. As the premium for RAID diminishes and RAID functionality can be acquired for little to no additional cost (such as with storage clusters), expect to see RAID more broadly used.

Certainly, a lot of reasons exist for moving to storage clusters. Nevertheless, the value for smaller, distributed sites (a major segment of video surveillance - banks, smaller retailers, QSRs) is not as strong.

Constraint #1: Not Effective for Smaller Camera Counts

Storage clusters have a startup cost that is notably higher than the internal storage DVRs/NVRs use. Just like any PC, internal storage is available by default and the only incremental cost is usually adding in the drives themselves. With a storage cluster, you usually have a separate appliance with electronics and computing infrastructure. As such, before you deploy any drives with a storage cluster, you first have to pay for this additional appliance.

With a storage cluster, the minimum available size seems to be 4TB at about $8,000 MSRP. If you use significantly less than 4TB, the cost for a storage cluster will be significantly higher than simply adding in drives to your DVR/NVR. Moreover, the benefits of pooling decrease because you are likely using less DVR/NVR units and do not need to worry about padding to achieve storage durations.

This is not trivial because large corporations have millions of facilities around the world that fit these characteristics. Until and if storage clusters can become more competitive at lower storage entry levels, the value for customers will be quite questionable.

Constraint #2: Not Capable of Centralization Across Distributed Facilities

Even though storage clusters have significant economic benefit for large amount of storage use, this is generally not feasible for aggregating storage from facilities across the country. To the credit of the vendors in this space, they have not made this claim. However, you do hear this from time to time by some in the industry.

Take a fast food restaurant with 1000 locations. In each location they probably have about 250 GB of storage (more if they are rolling out new systems). In total, that's 250 TB of storage (at least), which is quite significant. Hypothetically, they could save a few hundred thousand dollars if they could eliminate hard drives in the restaurants and just have one central storage cluster.

The problem is that you need significant amounts of bandwidth to accomplish this that simply is not available to most sites. For 8 or 16 cameras, you might need 5 - 20 Mb/s in upstream bandwidth. This is a huge amount for most stores where DSL/cable modem is the norm. In other words, the cost of bandwidth is far higher than the cost of storage. As such, this is not very realistic.

Conclusion

Driven by price competitiveness and a number of significant advantage, storage clusters will quickly become a major force in sites with modest to large numbers of cameras. Nevertheless, the sizable segment of the market with small camera counts per site will not see significant advantages in this. All integrators and security managers should carefully track and learn more about security clusters so they can take utilize their significant advantages.

Chapter 19: The Value of Centralized Video Analytics

Performing analytics at the DVR/NVR is a very popular choice in video surveillance. Reading the trade magazines and viewing marketing materials, you probably would not think so because 90% of the attention goes to analytics at the edge.

To me, this is a classic case of what vendors want the world to be rather than what is best for customers. For many customers, centralized analytics are a far better choice. Here are the top reasons:

- Reuses your existing cameras.
- Less expensive than analytics at the edge.
- Simplifies maintenance and upgrade of analytics.

Reuse Existing Cameras

Customers, justifiably, hate to throw away usable assets. The problem is that to use smart cameras you will generally have to throw away existing assets or purchase new assets that are redundant. Over 80% of cameras deployed are analog - none of them support analytics. You will either have to replace them or add an encoder with built-in analytics. Furthermore, most of the IP cameras do not have the capability to be upgraded to video analytics. As such, even if you deployed new IP cameras 6 months ago, those too would have to be replaced (perhaps you can relocate or resell those cameras).

You may be in a situation where you are adding new cameras or are ready to throw away existing cameras. In that case, great. This is not a problem. But most people are not in that situation.

Less Expensive

Consolidating video analytics at the DVR/NVR reduces cost. Smart cameras are usually a few hundred dollars more than traditional IP cameras. Smart DVRs/NVRs (systems that consolidate analytics and video recording in one) are usually no more than a thousand dollars more than a DVR.

Here's what happens. If you buy a smart DVR/NVR you pay about a thousand dollars more. If you buy smart cameras and need to replace your existing cameras, you can easily pay $5,000 to $15,000 more. Even if you do not have to throw away existing cameras, it can cost you a few thousand dollars for the premium of smart cameras.

Fairly small companies like Clickit and i3DVR are being selected by many customers for just this reason. They have built DVRs with analytics inside that only cost modestly more than a traditional DVR. The economics are such that this is obviously very attractive and despite the fact that these companies do not have big marketing dollars, there are getting some impressive wins.

Simplifies Maintenance and Upgrade

Not a lot of people are talking about this yet but maintenance and upgrade are going to be very problematic with smart cameras. Smart cameras are shiny today but in 3-5 years, your smart camera is going to look like the first generation iPod - big, bulky, stupid and uncompetitive with the 2011 state of the art. It's not practical to replace the chips inside each camera where it is very practical to upgrade a centralized server than handles analysis for numerous cameras.

Conclusion

While I am not opposed to analytics at the edge, the radical imbalance of coverage and treatment of this issue is a disservice to security managers. Hopefully, this article helped to shed some light on the oft-overlooked benefits of centralized analytics.

Chapter 20: 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 your 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 21: 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 clearing 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 to 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.

Chapter 22: Introduction to City-Wide Surveillance

While the publicity goes to mega-cities deploying video surveillance, city wide video surveillance is becoming very cost-effective, valuable and viable for 'normal sized' cities throughout the world.

The media coverage for the New York and Chicago city deployments can make city-wide video surveillance seem daunting. It appears that you need:

- Tens of millions in funding
- Homeland security grants
- Defense contractors
- Deploying complex new wireless networks
- Integrating military style command and control systems

In reality, though, most any city can benefit from mature, inexpensive and flexible city wide video surveillance.

The City of Longmont, Colorado provides a nice example of how to deploy city wide video surveillance. Over the last few years, Longmont (population 71,000) has developed a first class city wide solution. Working with Volpe Industries and using video surveillance solutions from Axis Communications and Detexi Systems, Longmont now has a powerful surveillance solution.

This article explores some of the key principles used in this deployment to build a successful city wide surveillance system.

Principles for Success:

1. Use Existing IP Networks that the Municipality Manages
2. Deploy NVR servers at Facilities Throughout the Facility
3. Use Direct Wireless Links to Connect Camera to Facilities
4. Share Video from the City with the Police Department's Command Center

5. Expand the System Step by Step, Year by Year

Principle 1: Use Existing IP Municipality Networks

Most cities manage their own internal networks for city facilities. These networks are a simple and low cost way to build a city wide surveillance system. These networks generally connect city facilities across the municipality and often provide high speed connectivity, to boost.

The integrator, Volpe, worked closely with the Longmont's CIO to put the IP video surveillance system on the municipalities network. The incremental cost of adding the system was practically nil as it leveraged this existing infrastructure.

Principle 2: Deploy NVR Severs at Each Facility

For each facility using IP Video Surveillance (e.g., libraries, schools, city hall, police stations, etc), an NVR server was deployed to store and manage video from the local cameras. This takes advantage of video being recorded much more often than it is viewed. While video must be streamed from the cameras frequently or constantly to enable recording, only occasionally does the video need to be viewed by city officials such as the police. Placing an NVR on each site significantly reduces the amount of bandwidth needed on the municipalities network that connects different facilities. This is important in making the addition of video surveillance as low impact as possible on the municipalities networks.

While centralizing video storage offers some savings in server and storage consolidation, like most organizations, Longmont benefited more from minimizing the impact on the city's network.

Principle 3: Direct Wireless Links from Facilities

A number of outdoor locations needing surveillance were economically addressed through direct wireless links originating from city facilities. From the roof of city facilities, wireless links were established to various points of interests within a few miles from the facility. As these connections were direct (point to point or point to multipoint), they were rather inexpensive and simple to establish.

Principle 4: Share Video

The hundreds of cameras now deployed across the city can now be leveraged by the police to help respond to emergencies or critical investigations. By using the city's IP network, the Police can access any of the NVR servers in the city to view live or recorded video. This has already helped handle real time incidents as well as solve cases where criminals have moved across the city.

Principle 5: Expand Step by Step

While city wide surveillance is often thought of as a massive project, Longmont demonstrates that the system can grow incrementally. Indeed, at Longmont, new facilities have been coming on line every year for the last couple of years.

This allows city wide surveillance systems to grow in small chunks requiring tens of thousands of dollars rather than millions of dollars. By leveraging the city's LAN and deploying surveillance at city facilities and their surroundings, step by step, the city can grow the system. This can be quite valuable in budget allocations and in building public support for the value of the system.

Future Considerations

Citywide video surveillance systems can and will continue to grow. While Longmont is a great example of leveraging your existing resources and starting with simple, high value uses, city wide video surveillance has the potential to expand to address other concerns. Below are an example of those future considerations:

- Interfacing with Local Business NVRs/DVRs: A lot of interest exists in sharing video between cities and local business to help respond to crimes or disasters. This requires support or interaction with many different manufacturers of NVRs/DVRs. Currently, Longmont, like many municipalities has standardized on a single NVR platform from Detexi. This provides great simplicity as all cameras are managed by this system. Nevertheless, it is common that one manufacturer's NVR cannot access or view camera's from another NVR system. Command and Control systems can be put in place to access multiple NVR systems but this can significantly increase cost and complexity.

- Using Non-City IP Networks: Some facilities and some points of interest are not served by the City's IP Network. In those cases, the use of DSL or cable modem from the local telecommunications providers will be necessary. This will require some added complexity to provide security, etc. but is increasingly becoming an accepted and straightforward part of city wide surveillance systems.
- Provide Broader Camera Coverage: In some cases, cities want to deploy cameras in places where there are no wired networks and direct wireless connections are not feasible. Wireless mesh networks are an ideal solution to this problem. They are designed to handle obstacles, provide greater redundancy and cover broader areas. Nevertheless, they also are more complex to design and more expensive to deploy.

Conclusion

With IP video, city wide video surveillance is becoming an affordable and valuable way to improve security. By following the principles of Longmont's deployment, most cities can quickly and fairly simply roll out city wide video surveillance systems that provide a strong foundation for continuous improvement and new benefits.

Chapter 23: Is Public CCTV Effective?

While we continue to spend more on public CCTV systems, the debate on CCTV effectiveness has reached a polarizing and inconclusive standoff. On the one side, you have a number of studies and leading thinkers who clearly contend that CCTV systems are ineffective. On the other, you have numerous municipalities who are weekly green-lighting new CCTV projects.

This report offers key findings from the 20 top studies/articles in the field and offers practical recommendations on how to optimize the use of public CCTV systems.

Key Findings Summary

- The expectation that CCTV systems should be deployed to reduce crime rather than solve crime has created huge problems.
- While the studies show serious doubt on CCTV's ability to reduce crime generally, a strong consensus exists in CCTV's ability to reduce premeditative/property crime
- CCTV is consistently treated as a singular, stable technology, obscuring radical technological changes that have occurred in the last 10 years
- Differences in per camera costs are largely ignored, preventing policy makers from finding ways to reduce costs
- Routine comparison of police vs cameras is counterproductive

Practical Recommendations Summary

- Stop claiming that CCTV can generally reduce crime
- Optimize future public CCTV projects around crime solving rather than

crime reduction

- Optimize future public CCTV projects around material and premeditative crimes
- Target technologies that support crime solving and material/premeditative crimes
- Focus on minimizing cost per camera

Finding: Crime Reduction vs Crime Solving

The overwhelming majority of studies focus on analyzing CCTV's ability to reduce crime. The general approach is to take current crime statistics for a region and compare those statistics to the period after installation of CCTV. A number of techniques are used to adjust to control for general changes in crime and to track displacement or diffusion of benefits to other areas. Nevertheless, the focus of all quantitative analysis has been on reducing crime.

This is the mirror opposite of the private sector. In the private sector, the overwhelming majority of CCTV systems are justified by their use in solving crime. It is investigations where most private businesses find value and return in their CCTV systems. For businesses, only a very small percentage of CCTV cameras are ever even watched. The systems pay for themselves by periodically being able to identify or prove a criminal activity.

This indicates a failure of expectations for public CCTV systems. In the private sector, when CCTV effectiveness is discussed, the assumption is usually that CCTV is used for investigations. By contrast, the focus on public CCTV effectiveness being determined on reducing crime sets a dangerous expectation that is difficult to achieve and likely to create dissatisfaction within the community.

The problem seems to be the fault of the original advocates of these systems, rather than a deficiency of the testers. The academics and researchers performing these tests were reacting to the expectations that the proponents of these systems made originally.

In the recommendations section, I will examine how we can move beyond this unproductive and problematic situation.

Finding: Reducing Crime Generally vs Premeditative/Property Crime

The media's main focus has been on whether or not CCTV reduces crime as a whole. This often has turned the issue into an all or nothing debate. The testing has also focused on the general impact on crime reduction but notable attention has been paid to different types of crime.

Widespread consensus exists that CCTV is effective in reducing premeditative/property crime. All the studies acknowledge this, even the ACLU's which otherwise is extremely negative towards CCTV. The most frequently cited example is the ability to reduce thefts in parking lots.

By contrast, the same studies widely agreed that CCTV demonstrated little or no affect on reducing crimes of passion. Incidents like public drunkenness or acts of rage generally did not seem to be affected by the presence of CCTV cameras.

This fits a broadly accepted rational actor model and the effect that CCTV cameras has on rational actors. Since CCTV cameras increases the risk that a criminal will be prosecuted for a crime, the criminal will respond accordingly. The cameras will affect the perceived risk/reward calculation. Common sense indicates that this impact is much more likely for property/premeditated crimes than it would be for crimes of passionate, where by definition, people are not calculating the consequences.

Rather than engage in political debates over the issue in general, we should use this more nuanced knowledge to optimize our use of CCTV.

Finding: CCTV as Singular, Stable Technology

The studies overwhelming treated CCTV as a singular, stable technology. Only the UK Home Office Report of 2005 even acknowledged the issue of technological change. The rest of the studies do not even discuss differences in technology available. I do not fault them as the evidence available is limited to even conduct such a test. Nevertheless, differences in technology can make an extreme difference.

The studies cover a very broad time period. The oldest study I found was from 1994 with most of the studies available being performed in the period from 2000 – 2004.

The problem is that CCTV technology has experienced a dramatic transformation in that time period. This is somewhat similar to the type of change experienced with mobile phones going from big, bulky, limited and expensive to slim, powerful and ubiquitous. It is quite unfair to assess the question is CCTV effective, in any form, without factoring in the differences in the type of technology used.

The examples found in the studies were fairly shocking compared to today's mainstream CCTV systems. The clear majority of systems employed in the studies used VCRs. Even when systems used DVRs, most were recording under 2 frames per second. All of the systems used standard definition cameras. While none of the reports discussed the type of transmission systems, given that almost all the tests were from 2004 or earlier, it is extremely likely none of them were using IP networks for transmission. Though limited, the best discussion on this topic in the literature is the 2005 UK Home Office Report.

While none of this is the researcher's fault, not factoring changes in technology obscures crucial differences. In the recommendations section, I explore what types of technologies and how they can impact system effectiveness.

Finding: Differences in Per Camera Costs Largely Ignored

While most studies cited general cost numbers, the cost per camera was largely ignored. The most frequently cited number is the amount the UK home office has spent on CCTV (500 million pounds). However, only the 2005 UK Home Office study actually broke down the cost per camera. Since the studies were focused on determining if the crime rate was reduced, this element is understandable. Nevertheless, communities could save significant money and improve effectiveness by more carefully tracking the cost per camera.

Understanding the cost per camera is important to recognize changes in technology and to identify waste. The 2005 UK Home Office report indicated that cost per camera ranged from $7,000 pounds to $33,000 pounds for cameras installed in the late 1990s and early 2000s. The study does not clearly explain the cause of the cost differences.

In my experience deploying similar systems, the main driver of costs from this era is the transmission systems. Because these cameras are generally outdoors and distributed throughout a city, transmission systems need to be built to send the video from the camera to the monitoring center. The solution of choice in this time frame was proprietary analog fiber transmission systems. Such systems required expensive transmission equipment and almost always laying of new fiber. This routinely generated costs of thousands to tens of thousands.

By contrast, today, the solution of choice for transmission is IP networks. IP networks dramatically reduce the cost of transmission. IP networks replace proprietary analog fiber systems with low cost commodity IP equipment. IP networks often can share existing fiber networks or connect to a telecommunication carriers system to greatly reduce or eliminate the need for new fiber or construction.

Finding: Cops vs Cameras Comparison Counterproductive

A frequent sentiment expressed by interviewees in both articles and studies is the preference for police officers versus cameras. While this is obviously understandable and I expect most every reasonable person would agree that police officers are preferable to cameras, this omits a crucial element.

Since police officers are so much more expensive than cameras, a comparison between the two is very misleading. According to the 2005 UK Report, the annualized cost per camera ranged from 600 to 3000 pounds. This is 1/15th to 1/80th the cost for a yearly police officer (including benefits, training, equipment, etc). In actuality, then the comparison is more like dozens of cameras versus an officer. Furthermore, given the significant price reduction in CCTV systems since most of the tests occurred, the comparison is now between hundreds of cameras and a single police officer.

Examined at a macro level, a similar distortion is apparent. Many of the articles and studies cite the 500 million pound UK Home Office spending over the last decade. Nevertheless, 500 million pounds for CCTV represents less than 1% of the spending on police officers during that time period.

Even if all funding on CCTV was transferred to hire new police officers, it would only increase funding by a very small percent. And, of course, a small percent increase in police officers would not be expected to dramatically decrease crime either.

This is an area where CCTV proponents have created unrealistic expectations that actually undermine their own cause.

Now, let's examine some recommendations:

Recommendation: Abandon emphasis on general crime reduction

Proponents of public CCTV systems should abandon the emphasis and claim that CCTV systems can reduce crime generally. Even if proponents ignore the fact that studies demonstrate this, clinging to this claim only creates greater debate and dissension.

By abandoning this claim, it will heal some of the major discord and allow all parties to focus on better uses of CCTV. Given the vastly improved quality of today's CCTV systems at greatly reduced prices, this should be reasonable to accomplish.

Recommendation: Focus Projects on Crime Solving

Just like the private sector has broadly adopted CCTV by focusing on solving crimes, the public sector should too. This would save communities money as certain features or cameras could be eliminated and designs could be focused on areas and technologies that help solve crimes.

This would simultaneously ease the impact on privacy as less attention and resources would be placed on trying to monitor systems live and thereby the risk of monitoring the innocent public.

Recommendation: Focus Projects on Material/Premeditative Crimes

To the extent that CCTV is used to support crime reduction, such efforts should focus on material/premeditative crimes.

Limiting the locations covered and monitored live to those areas with high rates of these types of crimes will maximize the probability those systems will be effective.

Recommendation: Target Technologies that Support Crime Solving

Though historically the camera of choice has been a PTZ, systems should emphasis the use of megapixel fixed cameras.

A PTZ, or Pan/Tilt/Zoom camera, can be controlled by an operator to look in many different directions and areas. PTZ cameras are favored by security operators as it allows them to control the camera in live monitoring. Two significant downsides exist for PTZs: One, they require a dedicated operator to use the cameras, incurring significant operation cost. Two, PTZs are generally bad for producing evidence because they miss everything expect for the area where the camera is momentarily positioned.

Megapixel cameras are far better fit for public places and crime solving. The cameras being used in the study are standard definition units with very limited abilities to view details. Much like the transition from film cameras to today's digital super high resolution cameras, CCTV systems now routinely employ megapixel cameras that provide dramatically greater detail. Such detail is key for public places that usually cover large outdoor areas. In this scenario, megapixel cameras give you the benefits of PTZ cameras because the detail allows zooming with the benefits of a fixed cameras' ability to always capture video of a set area. This is critical to crime solving because the camera needs to have an image if we are to use the evidence to identify or prosecute a crime.

Recommendation: Minimize Cost Per Camera

Given what we have learned from first generation systems and the advances in technology available today, we should be vigilant about tracking and minimizing the cost per camera. We now have a good sense of what works and does not work. We should optimize around that and ensure that we can keep costs per camera low.

The two key elements in minimizing costs is (1) ensuring that IP networks are leveraged and that (2) unnecessary funding is not spent for needless bells and whistles. By doing this, municipalities should easily be able to deploy systems for between 2,000 and 4,000 pounds per camera. This would drop the cost by 60% or more relative to historical standards.

Conclusion

With our extensive experience and knowledge, we must re-position goals, modify designs and economize our efforts:

- Set the goals appropriately on tasks that can succeed: Crime Solving and Property Crime Reduction
- Select technologies such as IP and megapixel cameras that improve performance
- Ensure spending per camera is controlled and benefits from new technologies

With these practices, we can ensure both effective CCTV systems and a positive economic contribution to society.

III

Evaluating New Products

Chapter 24: 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 25: 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 standout 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 26: 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 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 advertise 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:
John Honovich
(646) 867-1965
jhonovich@ipvideomarket.info
IPVideoMarket.Info