Security Manager's Guide to Video Surveillance

Version 1.0 / June 2008

John Honovich
IPVideoMarket.Info

Contents

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.

Can I Share this Book with Others?

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

Will this Book be Updated?

Yes, this book will be updated every 1 or 2 months 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.

Can 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: 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 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 appliance. 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.

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 product as software only. That is to say the NVR provides the user with a 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, offer appliances that offer the potential of reducing setup and installation complexity. On the large scale, companies such as Steelbox offers appliances that offer 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 failover 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 between 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 2: Introduction to Video CODECs

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 tradeoffs 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 losses 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. Evey 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 can 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.

Chapter 3: Bandwidth Basics for Video Surveillance

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

How Much Bandwidth is Available?

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

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

	Bandwidth Generally Available
Same Building	70Mb/s to 700 Mb/s
Different Buildings	.5 Mb/s to 5 Mb/s of

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 becomes generally becomes very expensive. In most locations, getting 10Mb/s of bandwidth can cost thousands per month.

Many talk about fiber (sometimes called FTTH/FTTC) but fiber to the building is not and will not be widely available for years. Fiber to the home 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 are low because there are minimal to no construction expenses. When you are building a network across a city, you need to get rights of ways, 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 by 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 4: Examining Video Analytics

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

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

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

Top 3 Problems:

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

Eliminating False Alerts

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

Most are familiar with burglar alarm false alarms and the frustration these causes.

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 a often overlooked and somewhat hidden issue in video analytics.

Over a period of weeks or months, 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 get put to the side 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 system 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 systems 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, so much of the first generation video analytic deployments, came from government grant money, essentially making the 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 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.

Chapter 5: 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 4CIF standard definition video. 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 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 is a lot of advanced details that need to be set correctly.

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 reutilizing 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 booth 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 6: Introduction to DVR/NVR 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 strorage 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 7: 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 that wireline 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 can 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 has significantly less bandwidth the wireless system states. 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 seriously 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 challenges. 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 unjustifiable. 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 success wireless video surveillance systems.

Chapter 8: 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 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 unknownable 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 in new functionalities. Other system depends on those APIs. 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: Your Stuck with what the API does

Unless your 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 undoubted ably grow. Understanding the realities of using APIs will ultimately help us maximize our value of system integration.

II

Examining Key Trends and Emerging Products

Chapter 9: 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 IoImage 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.

IoImage is showing us the future of advanced IT technologies in the physical security space. Let's contrast what IoImage 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 IoImage products from? Northern video and now, SuperCircuits. That's right, SuperCircuits -- The magazine you get with the $12.95 pinhole spy cameras now offers IoImage 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, IoImage is making it easy. IoImage is making it so easy that it's reducing the need for IT to be involved. IoImage let's the security manager concentrate on meeting his security goals. So while Cisco and IBM may be friends with the CIO, companies like IoImage 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 10: 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 Integrator's Skills

Many underestimate the importance of security integrator's 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 that 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 11: 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 matrixes, 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 dection, 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 IoImage 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 12: 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, main 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 hybid. 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 13: Performing Analytics in Your DVR

Since so many security managers have DVRs, ObjectVideo's recent announcement could be a major factor in future video surveillance purchasing decisions.

ObjectVideo announced the ability to add their analytics to DVRs by a simple software upgrade.

For 3 years, smart cameras and software only NVRs have dominated the industry discussion. Boxes were widely regarded as dead. However, this announcement could 'resurrect' the dead and place a major roadblock in the paths of recent entrants.

ObjectVideo is not the first to support doing analytics in a DVR. This is not news.

What is so important here is:

1. ObjectVideo has distribution/partnership arrangements with almost every major legacy DVR manufacturer.
2. ObjectVideo has complete software integration with almost every DVR manufacturer.

This means, the ability to distribute and actually implement this solution is relatively straightforward. OV might not have invented analytics in a DVR but they have a very strong shot at making it mainstream.

This is great news for security managers and potentially seriously trouble for

software only / recent entrants.

This is not significant because of existing units. OV will probably not be able to add their analytics to existing boxes in the field, especially units deployed a few years ago. These boxes likely won't meet the minimum resources. It would be great for OV and legacy DVR manufacturers if they did but even without this, it's significant.

It is significant because it shifts the balance of power in purchasing decisions for second generations DVRs. Almost everyone has a DVR today so each account has an incumbent, usually Intellex, Kalatel, Verint, DM, Honeywell, March, Pelco, etc.

Customers have a strong incentive to continue with their existing DVR manufacturer. Not out of loyalty, but of basic economic pressure. The transaction costs of switching are high and to overcome them, a challenger needs to make a clear case for a significant advantage.

To date, this case was that adding analytics to existing DVRs was really expensive, making the switch to a new solution reasonable. Adding on a separate appliance to your DVR was very expensive. 4 years ago, you had to buy a separate box from ObjectVideo that could run $4,000 per channel. This was prohibitive for all but the most critical security scenarios. Alternatively you had to use smart cameras but those are expensive as well - commonly a few thousand dollars and requiring a swap out of existing cameras.

Now, customers can keep their existing cameras, not worry about switching client software and potentially lower their costs.

And, most of all, it does not really matter how well OV works relative to other analytics. As long as it is good enough, the ease of adding analytics and its

distribution with your existing system will win be sufficient.

Chapter 14: 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 interal 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.

Saving video from being lost is usually a nice to have for video surveillance. It is generally not critical because the probability of a incident being lost is usually low. This is based on my experience in government, military and Fortune 2000 companies. Video storage is generally more like insurance than it is like your children. If you lose your insurance for a few days, it's a risk but you are usually fine. Video surveillance storage is pretty much the same.

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 15: Megapixel Becoming Affordable with H.264

ArecontVision's release of megapixel cameras will spur adoption of megapixel cameras for mainstream security organizations.

Until now, bandwidth and storage costs were big problems so even if you were willing to pay the premium for the cameras, the total cost of the system was hard to justify. Now, with H.264 megapixel cameras, the total cost of megapixel camera systems drops significantly, making it easier to find the budget and justify the expense.

Advantages:

- Reduce costs: Lowers cost of storage by $1,000 or more per camera
- Eliminates barriers: Enables many more networks to support megapixel cameras

Disadvantages:

- Using analytics with these cameras reduces the H.264 benefit
- Costs few hundred dollars more per camera

Potential Risks:

- As of June 2008, just became generally available
- Which and when will DVR/NVR manufacturers support the CODEC?

The central advantage of H.264 cameras is that they reduce the amount of bandwidth needed. ArecontVision is claiming a 5x - 12x reduction of bandwidth.

So, if your megapixel camera needed 10 Mb/s before (with MJPEG), it might now need only 1.5 Mb/s. So for each camera, you will save a lot of bandwidth. I am going to choose 3 Mb/s to be conservative. (To read the details see footnote #1 at the end)

Reducing camera bandwidth by even 3 Mb/s per second can save thousands per camera.

Let's say you want to record video for 1 month, a fairly low storage duration for today's security manager. That 3 Mb/s would require an extra 1000 GB of storage. Now, storage is getting cheaper but that much storage, per camera, can cost you an extra $1,000. Imagine if you wanted a 16 channel megapixel system, that's $16,000 more just for the storage. Big money for most of us.

You also get a similar benefit on the network side. Most of us are reluctant to spend major money on network upgrades to support video systems. The hope is that you can use existing networks or simply purchase low cost, basic networking equipment to get the video from the cameras. Historically this has been a very tough challenge with megapixel cameras. With megapixel cameras routinely needing 5 Mb/s, 10 Mb/s, 20 Mb/s or more, the load was very high.

H.264 is like getting a free upgrade from dial-up to broadband. The massive savings in bandwidth let's you do things that were previously prohibitive.

You will get this benefit both for wired and wireless networks. With wired networks, you likely can add many more megapixel cameras without hitting problems. With wireless networks, for the first time you might be able to use megapixel cameras.

So what's the risk and downside?

The Arecont cameras will not support analytics (footnote 2 for details). So, if analytics are driving your decisions, these cameras don't fit. However, for your analytics needs, consider using standard definition IP cameras and using analytics on these. For most scenarios, this will give you the alerting you need, complimenting nicely with your higher definition H.264 cameras.

The Arecont H.264 cameras will be more expensive, likely a few hundred dollars more. However, this should be easy to justify because of the storage and bandwidth cost reductions, your overall installation cost should be cheaper.

The H.264 cameras are just starting to be released for general availability at the end of June 2008. As such, depending on when you read this, you may not be able to obtain the cameras yet.

Also as of June 2008, very few NVR/DVR manufacturers are supporting Arecont's H.264 cameras. Make sure that your video systems vendor will support and determine when they will support it. Given Arecont's wide distribution, low pricing and the economics of H.264, I believe this will happen fairly quickly but it could provide short term logistical problems.

In sum, H.264 is changing the economics of video surveillance system design, enabling security organizations to cost-effectively deploy megapixel cameras. As it is early, be cautious but start evaluating and making plans for deployment.

Footnotes:

1. ArecontVision is claiming an average of 10x bit-rate reduction for their H.264 compared to MJPEG. Let's be conservative and say it's only 5x. So

a 2 Megapixel camera using MJPEG that might consume 20 Mb/s is 4 Mb/s with H.264. Let's also assume that different camera settings could reduce the average bit rate to 10 Mb/s for MJPEG. Let's say in both scenarios we other advance configurations that reduce bandwidth equally by 50% bringing us to 5 Mb/s for MJPEG and 2 Mb/s for H.264. Even in this conservative scenario, that's a reduction of 3 Mb/s per camera.

2. Performing the analytics at your NVR/DVR is unrealistic. The processing cost to decode H.264 will be fairly prohibitive. You could consider using multiple streams, 1 with H.264 for recording and 1 with MJPEG for analysis, to get both. The bandwidth is higher obviously but it at leasts eliminates the storage issue and allows for analysis with this camera.

Chapter 16: Simplifying Megapixel Surveillance

While megapixel cameras are a 'hot' technology, a number of factors including cost, complexity and usability undermine its uptake. Megapixel cameras still represents less than 1 or 2% of the total security cameras deployed despite its accelerating growth. As such, for megapixel cameras to go mainstream, a number of issues need to be resolved.

While Avigilon is best known for its super high definition cameras, its most important impact may be in solving critical problems that constrain megapixel cameras from being used in the mainstream market. For megapixel camera deployments, Avigilon may be able to reduce total system costs by 20% to 35% relative to leading megapixel/NVR alternatives while increasing the overall system usability.

Summary of Recommendations

- If you are evaluating a new DVR/NVR and are interested in megapixel cameras, you must seriously consider Avigilon.
- If you are a large enterprise organization with demanding needs for third party application integration and advanced domain specific functionalities, you must verify with Avigilon directly if they can meet all of your requirements.

In this report we will be examining the advantages and risks of the Avigilon offering to explain the recommendations we offer.

Advantages Overview

- Improves Image Quality Significantly

- Reduces Cost of Megapixel Cameras and Storage
- Increases Usability of Viewing and Investigations
- Makes System Integration Simpler

Risks Overview

- Benefits from Avigilon are maximized when using megapixel cameras. If you do not plan to use many megapixel cameras, obviously, Avigilon's business case is reduced.
- Avigilon is not scheduled to support other manufacturer's IP cameras until early 2009 and it will be limited to only the top selling models.
- Certain advanced video management features are still in development and you will need to verify with Avigilon on these points.

Avigilon Overview

Avigilon supplies a full suite of video surveillance products including cameras, encoders and a video management system. Cameras range from standard definition to 16 MP units. Encoders enable support of fixed and PTZ analog cameras. The video management system is offered both as an appliance and software only versions.

Most importantly, all of the Avigilon products are designed to work together as one integrated system. This is significantly different and perhaps a unique approach in the IP Video Surveillance market. Whereas it is common that you can buy a megapixel or IP camera from dozens of manufacturers and use it with dozens of NVRs and DVRs, Avigilon's cameras and encoders are designed to only work with their NVR.

Avigilon's reputation is based on superior image quality, however, the greatest

strength of the solution comes from it being an integrated system. With an integrated system, the manufacturer can ensure that the product works optimally from end to end, simplifying integration and increasing usability. They can also reduce costs by streamlining functionalities. By contrast, with an open system, common in IP video surveillance, the component manufactures have much greater difficulty coordinating, simplifying and ensuring the product works optimally end to end.

This approach drives both Avigilon's strengths and risks.

Advantage: Reduces Costs

Avigilon significantly reduces the costs of cameras and storage.

On the camera/encoder side, here are 3 examples:

- The MSRP pricing for a 1 MP camera from Avigilon is 20-40% lower than the MSRP of the inexpensive and popular ArecontVision av1300.
- The MSRP for a 5 MP camera from Avigilon is under $1000 comparable to ArecontVision's pricing and hundreds of dollars lower than other top megapixel cameras.
- The MSRP for a 4 channel 4CIF/120fps encoder from Avigilon is 33-55% lower than the top competitors MSRPs for equivalent encoders.

The cost advantages arise from the tighter integration of cameras, encoders and management software and the ability to bring intelligent video features server side and avoiding more expensive compression technologies such as MPEG-4 and H.264.

For storage, Avigilon's built in “data aging” can significantly reduce storage costs. Essentially, Avigilon creates three buckets of storage – new, older and oldest. New

video is recorded at full frame rate. Older video is reduced to half the new video frame rate while the oldest video is reduced to one quarter the new video rate. User configurable, typically the new video bucket is held for a few days to capture any incidents that may happen over a long weekend; the older video bucket is held for a number of weeks for general investigations and the oldest bucket can be held for any number of months or longer for insurance purposes. This ensures you always have the highest quality evidence available while reducing storage costs by 50% or more.

While data aging is offered in some form by a number of DVR/NVR vendors for standard definition cameras, this is not common for megapixel cameras. As such, it is a significant advantage, especially given the high cost of storage in megapixel camera systems.

Advantage: Increases Usability

While camera resolution have increased dramatically, the amount of bandwidth going to one's office or home has grown very slowly. This increasing disparity is creating a very significant usability problem for most megapixel video surveillance systems. If you want to watch video but the video streams are too large for your connection, you are likely to have a very frustrating and poor experience.

Most video surveillance monitoring scenarios are affected by this disparity. This applies when either you or the NVR you are connecting to, uses a DSL or cable modem type connection. With so many NVRs at branch offices and so many people viewing remotely, the odds are that this issue will affect you. Indeed, unless you and the system you want to view are in the same building or campus, it is likely this will be a problem.

Avigilon's approach to transmitting and encoding video allows for much higher usability than leading megapixel solutions. Avigilon uses JPEG2000, the second generation version of the underlying CODEC used by other megapixel cameras (JPEG/MJPEG). JPEG2000 provides significant advances in transmission and dynamic changes to resolution displayed. This offers critical benefits to usability as it can radically reduce the amount of bandwidth consumed while delivering the exact level of quality and detailed wanted by the user.

Let's say you have a 5 MP camera covering a parking lot. If you are looking at the full view of the entire parking lot in quad view on a standard 1280x1024 monitor, sending the entire 5 MP image is a waste. With 90% less pixels on your display, you can send just 10% of the image data and it will look the same to you on your monitor. Only when you zoom in to a specific region do you really need more pixels in a certain area and the Avigilon NVR dynamically handles which parts of the image to send. With MJPEG, on the other hand, the conventional way megapixel cameras are streamed, all 5 MP is sent to your PC which unnecessarily uses large amounts of bandwidth. The PC then must select the area you zoomed in on and discard the rest. By contrast, with Avigilon, only the required pixels of the 5 MP images are sent to your PC. By only sending the minimum image data required, image quality is improved, bandwidth is greatly reduced, and interacting with the Avigilon user interface is much more responsive making it easier to monitor cameras or to conduct investigations.

Advantage: Simpler Integration

Because Avigilon has developed an end-to-end system, they can ensure that the cameras and video management software work smoothly and reliably. Here are a few advantages:

- Avigilon servers can automatically discover and synchronize its cameras, saving integrators time and complexity when deploying the system.

- All of Avigilon's camera functionalities are supported by Avigilon's management software. This is rarely the case with other megapixel cameras. While megapixel cameras can offer dozens of functionalities, many NVR / IP Video solutions only support a fraction of those functionalities. Avigilon eliminates these potential implementation problems and hidden issues.
- When Avigilon makes changes to its cameras or management software, Avigilon can ensure the whole system works optimally with ease. This is more difficult when dealing with separate vendors for cameras and management software because coordination is complex and time consuming.
- Avigilon's partner portal offers excellent on-line tools that makes it very simply to design and specify the entire system (both cameras and servers), reducing complexity, error and time in putting together systems.
- “One Throat to Choke”: With Avigilon, any camera or management software problem is Avigilon's responsibility because they provide both. This is not to say that other suppliers would shirk responsibility. It's simply harder to determine which supplier can fix your problem when your solution has multiple suppliers involved.

With the advantages examined, let us look at the three main risks.

Risk: Mainly Analog Deployments

Clearly, Avigilon's strengths are built around its image quality and ability to simplify megapixel video surveillance. To the extent that you are not using megapixel cameras or only plan to use a small fraction of megapixel cameras, Avigilon's advantages are reduced.

Risk: Constraints on IP Cameras Used

The most serious risk with using Avigilon is the lack of support for other IP and megapixel cameras. The higher performance, ease of deployment and greater ease of use that Avigilon delivers comes from managing its own cameras.

To address this concern, Avigilon is scheduled to release support for leading IP cameras in early 2009. For most people who do not have IP cameras yet, this will not be an issue. For those who do, you should factor this in.

Risk: Limited Enterprise Video Management

As a relatively young company, Avigilon does not yet have as broad a suite of functionalities as some of the older and larger DVR/NVR providers offer.

Specifically:

- Avigilon currently does not support access control integration. They are scheduled to release Lenel integration in Fall 2008 in addition to their current support for triggers from 3rd party applications. If access control integration is a requirement, you should verify if they support your system or how they could support it.
- For advanced video analytics, Avigilon currently only supports LPR. Object recognition and face recognition are only available to select customers for beta trial periods and are only scheduled to be released at the end of 2008.
- Avigilon offers centralized management of all servers, supports LDAP and can perform redundant recording and archiving, however, Avigilon is not scheduled to have single-sign on until until 2009.

As is standard for a younger company, all of these elements are being developed but if you depend on any of them, you or your integrator need to contact Avigilon directly to get the latest timing on when and how they will support these elements.

Conclusion

Avigilon offers a very different and very powerful way to deliver greatly improved image quality while reducing the cost, complexity and usability concerns of deploying megapixel cameras.

Chapter 17: 360 Panoramic Cameras Going Mainstream

After years of unfulfilled promises, panoramic cameras look ready to go mainstream. Increased performance, reduced costs and the rise of IP video systems have transformed a product with great potential into a key component of video surveillance systems. Now that its implementation has caught up, expect to see panoramic cameras deployed widely.

Many of you, including myself, are skeptical of this technology. Though panoramic cameras have won ISC West "Best in Show" Awards twice in the last decade, they have never been a big commercial success. First, the IPIX CommandView360 won the award. Then, IPIX, very famously, crashed and burned. Then, in 2006, Capture Omniscape won the same award. This camera has become a promising niche player but certainly not a mainstream powerhouse.

Now, Grandeye has unveiled a new pure IP panoramic camera series that has the potential to change how IP security systems are designed. Grandeye has been developing panoramic cameras for the last 5 years and is the OEM behind the cameras offered by Sentry360 and Capture Omniscape.

Grandeye offers a 5 MP, 360 degree camera in a small, discrete form factor for an MSRP under $2,000 that can be integrated into mainstream NVRs/DVRs. This clears the major operational issues that panoramic cameras suffered in the past.

The images above depicts the camera itself and demonstrates how discrete the camera is when installed.

With this, panoramic cameras become a smart choice for:

- Providing detailed identification of people in a ~ 1,500 sqft / 150 sq meter area like retail displays, hallways, lobbies, meeting rooms, exits, waiting areas, etc.
- Providing action identification in a ~ 15,000sqft / 1,500 sq meter area in warehouses, supermarkets, large lobbies, malls, etc.
- Replacing 3 or 4 cameras in an indoor open area with a single panoramic camera

In indoor facilities, like the areas mentioned above, panoramic cameras can provide the best solution for somewhere between 15% and 30% of all cameras. As such, it should become a standard part of video surveillance designs.

In the rest of this review, we will explore the details about the evolution of this

product category and best practices for using them.

How the Offering and Market Matured

Despite the hype for IPIX in 2003-2004, panoramic cameras suffered from 3 major problems.

1. The cameras were much more expensive than comparative cameras at that time.
2. The cameras were not supported by any of the mainstream video management systems at that time.
3. The video quality was poor relative to cameras at that time.

Five years ago, the video surveillance world was different and panoramic cameras were just not good enough. To use an IPIX camera meant using a stovepipe system that could not be integrated with your main video surveillance system. Most security managers are very reluctant to do this because of performance and cost issues. Moreover, even though the cameras offered 1 or 2 MPs, over a 360 degree image, the video quality was clearly worse than simply using 4 analog cameras. As such, the motivation for most was minimal and the obstacles were high.

Because of these fundamental strategic problems, IPIX's rampant marketing campaigns only made things worse. I remember going to IPIX booth multiple times not understanding what all the fuss was about. With companies like Axis and Milestone still trying to make their way to the mainstream, IPIX was a strange beast. Many people, especially with the spectacular collapse, felt the same.

Wider deployment of panoramic cameras started in 2006 with the release of a 3 MP "Analog series". With this system, the resolution increased to 3 MPs and it could be used with traditional analog systems. However, it requires its own recorder and could not be seamlessly integrated into IP video systems. As such, customers started to use this as a niche tool (especially in retail) to address high loss issues. This will be useful for organizations committed to existing DVR systems but less compelling for the emerging IP video market.

With the new IP offering from Grandeye, the offering is optimized for mainstream IP systems:

1. The MSRP is now under $2,000, in line with other 5 MP cameras.
2. The camera can now stream MJPEG over IP networks to any hybrid DVR or NVR.
3. The image quality is now up to 5 MP, providing strong quality even over 360 degrees.
4. The camera is designed for easy and concealed deployment in ceilings.

With this resolved, panoramic cameras start making sense for widespread use.

Best Practices for Using Panoramic

Panoramic cameras address a number of key problems in video surveillance:

1. Traditional camera deployments leave significant blind spots
2. It can be difficult to track suspects across cameras
3. Using multiple cameras in an area are often necessary but expensive
4. Multiple cameras generate aesthetic problems
5. Large camera counts can make customers feel uneasy or uncomfortable

Traditionally, detailed identification of people in anything other than a small, well defined, area (like a doorway) was very hard. With panoramic cameras, in rooms or areas under 1,500 sqft, it now becomes possible to get those details anywhere in the room. This helps solve more cases by ensuring not only evidence available but the evidence has sufficient quality.

Likewise, in large areas, investigators are forced to piece together an incident across multiple cameras and through gaps in coverage. With a 5 MP panoramic camera, the investigator can see the entire facility with sufficient detail to track a suspect or an activity across very large areas. This makes solving cases easier and allows many cases to be solved that would otherwise be inconclusive because of gaps in video coverage.

Panoramic cameras fill an important gap in the role of traditional Megapixel cameras. Traditional Megapixel cameras are optimized for wall mounting to look in a particular direction. This is great when you are looking for something specific (i.e., just people coming in a door or license plates at a car entrance). However, when you need to see a whole room, traditional Megapixel cameras force a trade off of which direction you want to see. Panoramic cameras eliminate this trade off.

As such, panoramic cameras provide an improved solution in monitoring hallways or multiple entrances to a room. The panoramic camera can replace multiple cameras looking down and across hallways. Likewise, it can eliminate the need for multiple cameras to cover different entrances to a room.

Nevertheless, panoramic cameras compliment other cameras and do not provide value in certain applications:

1. For capturing a single point or object. If there is a well defined area you

want and the rest is unimportant, panoramic cameras might be a waste and you can get higher quality by aiming a narrow angle lens at the target.

2. Monitoring large, dark outdoor areas. Because it is a 360 degree fixed camera, you will not be able to zoom across large areas. Also, megapixel cameras have challenges with super low lighting levels. If you are monitoring a crowd outside of a store, this will work well. However, you should avoid using this for monitoring a poorly lit fence line.

You should be aware of and consider two panoramic alternatives to Grandeye.

1. Arecont Vision offers a unit with (4) 2 Megapixel cameras inside. It's called a 360 degree camera but it's not truly 360 as a blind spot exists in the center (looking straight down). It's also not truly panoramic because it does not allow PTZ across the 4 cameras that make up the unit. The Arecont Vision and Grandeye cameras are about the same price so the Grandeye's more advanced functionalities will make it the better choice for most applications.
2. Immervision offers 360 degree lenses that are designed to work with many manufacturers analog and 1.3 megapixel cameras. This has the benefit of using existing cameras and a lower cost. However, because of the far lower pixel count, the image will be much less detailed. As such, this could work for action identification but would be a poor fit for personal identification or camera replacement applications.

Finally, as DVR and NVR manufacturers have only recently started to add support, you must check to determine that your system can support (For instance, Cieffe, NICE, Videonext, VideoProtein, and Clickit currently support Grandeye). Because they are IP cameras and use standard MJPEG for compression, support should be straightforward but it is obviously important to determine support

before deployment. Two forms of support exist:

1. Basic Support - the DVR/NVR can display and record user selected sections of the panoramic image. This is good for live monitoring.
2. Advanced Support - the DVR/NVR records the whole panoramic stream and allows operators to pan,tilt and zoom in the recorded video. This is important for investigations.

Conclusion

Given the growing maturity of panoramic cameras, now is the time for security managers and integrators to start carefully assessing how and where these cameras can improve security and reduce costs in system upgrades or new deployments.

Chapter 18: Unique Approach to Intelligent Video

Most products you see today are modular solutions where you mix and match different products to build a solution. While modular solutions have benefits, sometimes a tightly integrated solution can better solve your key security concerns. Intellivid could be doing that in retail.

Intellivid offers a tightly integrated solution that potentially offers significantly greater value than today's leading DVRs/NVRs.

• For retail managers, the system merits immediate consideration.
• For security managers of primarily indoor facilities, the system merits monitoring for future use.

Integrated versus Modular Systems

Understanding the difference between integrated and modular systems is critical to appreciating why Intlellivid could offer a more powerful solution than incumbents such as March or Milestone.

The dominant trend in video surveillance today is the open or modular system. Open systems are prized for their ability to mix and match components from different vendors and to integrate any number of systems. It offers flexibility and extensibility to start small and add in new functionalities.

The major drawback of open systems is they limit how powerful a system can be. The open system must be designed to be modular, having clear interfaces to allow

other components to plug in.

When solutions are already good enough to meet customer's needs, open systems provide the best choice because they don't sacrifice performance yet provide much greater flexibility.

By contrast, when a solution is not good enough, customers generally obtain more value from an integrated system that maximizes the solution. For instance, the iPhone is so good is because its an integrated system. Despite its many restrictions on using 3rd party products, is widely regarded as the best phone available.

This is a well accepted tenet of technology strategy by Clayton Christensen.

Intellivid's Advantages

Today's IP/Video Analytic systems are not good enough yet to solve retailer's problems. Most retailers have huge losses from boosters, internal theft, shoplifters, etc. Retailers have major areas where operational efficiencies could be improved. Video analytics still suffer from major problems in false alerting, usability and integration that prevent them from being a major financial factor in most retailers. Plugging in a variety of analytics that may not work well individually nor as a system is a recipe for serious problems.

Intellivid has unique potential to more effectively reduce loss and improve operational efficiencies through an integrated solution. While the major retail incumbents such as March, Milestone, Genetec and American Dynamics move to a more modular, open approach, Intellivid has focused on delivering an optimized, integrated solution for retailers. It would be quite difficult for others to mimic or match Intellivid's offering due to the engineering challenges such a move would require.

Intellivid Functionalities

A common concern for retailers (and any organization with large footprints) is determining where people are moving or have moved throughout a facility. This can be critical for tracking a suspect or locating an individual. Intellivid uses analytics across cameras to predict the most likely camera an individual may be moving towards. A semi-automated process, the Intellivid system suggests likely cameras to the operator, allowing the operator to simply click on the individual to continue tracking. Intellivid can then generate a customized movie of the individual moving across a series of cameras, providing unprecedented speed and completeness in evidence processing.

Intellivid not only integrates analytics across cameras, it integrates the use of analytics across the system. This tight integration makes it easier for users to employee video analytics and more likely that they solve real cases.

As tracking suspects is a prime task of retail security, Intellivid's unique ability to enhance this offers significant operational and financial benefits. Watching video to establish cases can take many hours to accomplish. Indeed, many investigations are abandoned simply because it is too difficult and complex to investigate. Intellivid cannot only reduce the amount of time per investigation but it can solve cases that would have otherwise been too difficult to solve.
Moreover, the same cross-camera analytics can be used to provide rich data sets for business intelligence purposes.

Let's say you want to conduct a customer study to better understand the shopping experience of a certain target market. Built in to Intellivid, using the same cameras and system, operators can use Intellivid's tracking to quickly trace and build an end-to-end movie of the customer's experience. This is far cheaper than the traditional alternatives such as focus groups or installing dedicated customer tracking system.

Similarly, for employee review/training purposes, the same tracking can be used to quickly review and assess the activities of an employee. Determining whether an employee followed standard operating procedures or how an employee interacted with a customer across a store floor becomes a straightforward and solvable task. This could equally be used for tracking employees suspected of internal theft.

Finally, in addition to these unique attributes, Intellivid integrates a leading suite of video analytics for people counting, removed object detection, etc. While offering of these analytics have become commonplace, the quality of vendor's offerings can differ significantly. Intellivid's offerings can be expected in the top tier of performance as they have focused on multiple year in-house development of analytics for retail.

Intellivid Positioning/Pricing

Though Intellivid can be used as an overlay to existing DVRs/NVRs, most customers will maximize value using Intellivid as a fully integrated video management system that records, searches, alerts and analyzes video. Intellivid's per channel pricing ($750 per channel for an 8 channel edition available for purchase online) is at a significant premium to IP video management systems but in line with video analytic license charges. Since analytics are used and purchased on all Intellivid channels, the effective system price is likely $3,000 to $4,000 more per 16 channels (a significant but not outrageous amount).

Finally, Intellivid's ability to track across a facility and provide an optimized workflow for security investigators is significantly different than leading video management solutions and very hard for those solutions (given their architecture) to replicate.

What are the Risks?

If you are not interested in using analytics and simply want a basic recorder, Intellivid obviously is a poor choice. Many retailers, especially late adopters, will be fine with existing products. For them, Intellivid does not make sense. For everyone else, a few risks should be considered in evaluating Intellivid.

1. *How well do Intellivid's more integrated analytics work?*
The problems of basic video analytics are well documented. Given that Intellivid's analytics are harder, how well will they work in your environment? If they work poorly, that will eliminate the potential increased value. A careful assessment of its performance in your facilities is important.

2. *Does Intellivid have all the basic video management functionalities needed?*
Video management is a fairly mature field with dozens of functionalities required. Even relative 'newcomers' such as Milestone and Genetec have been building such features for 10 years. Intellivid is only 5 years old and is likely still finalizing the dozens of basic functionalities needed. You may find that certain must-have are not yet complete so review this carefully.

3. *How difficult is it for a security organization to secure additional budget?*
While certainly possible, anytime security requires additional funding, the allocation and approval process can be tricky and time consuming. Engaging store operations, IT and finance may identify new sources of funding but it can also create new barriers to closing the deal that would not be available if security was simply allocating existing budget dollars.

4. *What do you do about your existing system?*
If you are in the process of upgrading from first generation DVRs, justifying the

cost of migrating to Intellivid can be feasible. However, if you have recently deployed a NVR or second generation DVR, the financial justification could be much more difficult. While you can technically overlay Intellivid to another video management system, the cost and complexity of doing so is often not feasible for organizations.

5. *Will modular analytics that plug in to open NVR systems become as good as Intellivid's solution?*
At some point in the future, analytics will mature. The challenge here is that it is hard to tell when. I would not be surprised if maturity take another 5 to 10 years. Once maturity occurs, the benefits of open systems increase. Yet until that does, a system such as Intellivid might provide much greater results and savings than an open, less powerful system.

The Upside

Intellivid has a unique approach and has been developing the underlying technology for a number of years. As such, if the more advanced analytics do work and provide substantial value beyond point analytics, Intellivid could be poised to become a major player not only in retail but within 3 to 5 years other market segments with similar environment conditions.

Because of the differing architectural approach, none of the current leaders (March, Verint, etc) could match Intellivid on Intellivid's key differentiators. Intellivid reports that sales in the last 6 months have increased considerably. Normally, I would discount that as vendor hype but it is feasible that Intellivid has only recently closed the gap on fundamental functionalities and is now able to win head to head against the incumbents.

All in all, Intellivid's focus on building highly optimized integrated solutions

could have a major, unrivaled, payout to the forward thinking security manager and integrator.

Chapter 19: Understanding Cisco's Impact on Physical Security

Cisco is the most prominent figure in the move of IT into physical security. As such, it is quite critical to understand Cisco's impact. To help assess the impact, this article reviews Cisco's video surveillance products, positioning and pricing, analyzes their impact on the industry and concludes with recommendations

Overview

Cisco will be a minor force in video surveillance primarily selling video surveillance solutions into existing Cisco accounts.

Cisco cannot be dominant because their core strengths and product strategy are poor solutions to the key challenges of video surveillance. However, their product offering will be sufficient for large footprint facilities. Given their strong channel relationships and this fit, they will have some success.

The two key reasons for this are:

1. *Cisco's solution to the live video monitoring problem is fundamentally wrong.*
2. *Unlike routing or IP telephony, video surveillance does not play to Cisco's strengths*

Both of these reasons will be examined in depth following a review of Cisco's products, positioning and pricing.

Cisco Products

The Cisco solution is optimized for distributing video, which is different from most NVRs/DVRs. Cisco leverages their advances in networking by optimizing the use of advance network features and functions. Moreover, they have a strong solution for accessing video at any time from any place. To read a good overview of Cisco's video surveillance solution I encourage you to read the well written recently released Cisco Video Surveillance Manager Solutions Reference Guide.

Beyond the encoding and video management features typical of video surveillance, Cisco offers advanced functionalities for live video monitoring. Cisco offers a virtual matrix solution that enables sophisticated distribution of live video from many locations to many monitoring locations. To handle bandwidth constraints that routinely arise in sending video across wide area networks, Cisco offers proxy processes that can adjust frame rate and resolution to make video. This can be very valuable in allowing remote viewers access to video without overloading the network.

Cisco offers a host of network optimizations for maximizing video surveillance performance. Two of the most important are multicasting and quality of service. Multicasting has the theoretical ability to massively reduce bandwidth loads when numerous viewers are watching the same video stream (as might happen in an emergency). Quality of service optimization can help ensure that resources are available for video so that when security video is critically needed, bandwidth is available. Nevertheless, these optimizations require network devices that support these features (like Cisco routers) and expert configuration. If you do not have routers or switches that properly support this (which is common), you will need to upgrade.

Cisco offers its own IP cameras as well as supports many of the major IP cameras and encoders on the market today.

Though Cisco supports analytics and will certainly continue to expand, this is not a deeply integrated element in the Cisco video surveillance solution.

Cisco Positioning

This solution excels with large camera counts and a strong need for live video monitoring. Not surprisingly casinos are a good fit as they can have hundreds or thousands of cameras in a facility with dozens of operators viewing live video. The solution should also be attractive to municipal video surveillance solutions where large numbers of cameras are distributed throughout a city and where multiple agencies may need emergency access to video.

By contrast, this is a very weak solution for facilities requiring smaller camera counts. Even if you were an organization with thousands of locations across the globe (fast food restaurants, retailers), the necessity of using IP cameras or encoders plus setting up servers in each location make the solution very expensive and lacking in specific strengths for these deployments.

Cisco Pricing

Cisco's pricing is significantly higher than leading alternatives, both for products and services. For instance, the Cisco 2500 IP camera is almost double the Axis 210 ($800 vs $440 online pricing). Given the complexity and sophistication of the media server and encoding products, the video management components are likely to be much more expensive than alternatives from Genetec or Milestone. Finally, the services needed to optimize the network for Cisco's strengths are likely to add significantly to the overall cost. These costs will come both from the higher rates for network engineers and the additional time needed to optimize.

In all, I would not be surprised that a Cisco solution is 25-50% more expensive than leading IP based video systems. That being said, price is not everything and the return may be worth it.

With that in mind, let's analyze Cisco's strategic fit.

Cisco's Solution to Live Video is Fundamentally Wrong

Cisco has a clear solution to live video monitoring, a key challenge in video surveillance. The solution is to ensure organizations can get access to any live video from any camera at any time by optimizing network performance and video distribution. I believe this is the right problem but the wrong solution.

The live video monitoring problem will be solved by analytics -- not network optimizations making live video access easier. Since the live video monitoring problem cannot be solved by live video, Cisco is wasting huge resources trying to optimize live video. It's pulling them in the opposite direction of where the solution is emerging.

Even if you could make live video monitoring work from any camera to any location, it does not address the critical issue in security: how do you assess and identify threats? Most security organizations are uninterested in viewing lots of live video because they cannot make meaningful decisions based on it. While managing bandwidth is difficult and networks cannot easily support this type of live video viewing, this is at best a secondary concern.

While video analytics are still maturing, it is clear that only through video analytics, will the fundamental issue of live video be solved. Security managers are not so much interested in viewing live video as they are solving real time

problems. To the extent they can solve real time problems through analytics, that is the ideal solution to the live video monitoring problem. It is not a matter of if analytics are the solution but simply a matter of when and how analytics become that solution.

Of course, this does not mean live video monitoring will be eliminated. Rather analytics will mitigate the need to watch as much live video. For most security uses, typical video surveillance systems can meet the live video monitoring need even in an emergency by feeding 5 to 10 streams. For the very small number of security organizations that need even more live video feeds, other cheaper and simpler solutions can be found.

Though Cisco will certainly increase support for analytics, the system clearly is burden by costs for optimizing live video and is not designed for optimizing analytics. Moreover, Cisco will have adverse incentive to optimize analytics. Competitors will be much more determined to use analytics to reduce the importance of the network than Cisco. Because of this, I believe knowledgeable customers will see the Cisco solution as lagging and failing to incorporate the key technologies driving new value.

Video Surveillance does not Play to Cisco's Strengths

Cisco is so dominant in routing and IP telephony because it is very beneficial for customers to use a single supplier for those solutions. Though you can certainly mix and match networking devices, you increase the risk of interoperability problems. Also, since Cisco provides numerous advance features beyond the standards, if you elect to take advantage of them, it's not easy to integrate with 3rd party products. So once you have 1 router from Cisco, the value of getting all of your routers from Cisco increases (there is a network effect). Similarly, with IP telephony, once you have a Cisco Call Manager, you usually get the most

advanced and most reliable solution by using all Cisco phones. So while Cisco clearly offers strong solutions in these markets, what drives their dominance is that customers have strong incentives to buy the whole solution from Cisco.

In video surveillance, you do not get a lot of value from buying all your products from a single vendor. One router that has interoperability issues with other routers can become a major operational and financial problem for your network. By contrast, one camera that is not interoperable is simply an issue with that camera. Unlike routing, customers do not have strong incentives to buy only one camera type. The same point can be made for video storage. Similarly, we are seeing this trend in analytics with many analytics vendors co-existing and interfacing with different video management.

Even with video management systems (NVRs/DVRs), we are seeing command and control systems emerge to unify various DVRs and NVRs for global monitoring. This further reduces the value and importance of building a single end to end solution dominated by one vendor.

The point then is that even if Cisco was to have a strong solution, video surveillance solutions, unlike Cisco's current core markets, do not strongly motivate customers to standardize on one vendor's product.

Recommendations

While Cisco is certainly a strong overall company, it's video surveillance solution is credible but uninnovative. Like many other large companies (Bosch, Honeywell, Panasonic), they will win deals but they will not be a transformative force.

Be confident that Cisco is not transforming physical security. For most managers

with existing infrastructure, the cost of migrating to Cisco would be extremely high and the incremental value would be low. Keep focusing on new and innovative companies that want to make the network less of a factor in security by using analytics. It's through analytics and focused video surveillance solutions, that you will obtain the most efficient solution and an answer to live video monitoring.

Chapter 20: Should I Use My Router as a DVR?

Most organizations have routers so when Cisco announced you could plug a DVR/NVR into your router, many naturally became curious about using it.

Despite the great concept, Cisco's IP Video in a router solution will be uncompetitive and unattractive to most customers. The offering has serious flaws in features, applicability and pricing. (Disclaimer: I have previously written that Cisco has a weak video surveillance strategy. I think this will demonstrate examples of those problems.)

This reports overviews the offering, its advantages and disadvantages.

Advantages

- Eliminate Security Systems Integrator
- Attractive to customers with existing ISR routers that can support these modules
- Attractive to customers who are evaluating purchasing new ISR routers

Disadvantages

- More expensive than almost any NVR/DVR/IP Video software solution on the market
- Less Flexible / Expandable than software only IP Video solutions
- Mediocre Video Management capabilities compared to today's top solutions
- Deployable on only a small percentage on routers deployed

- Not realistic to deploy new routers simply to add video surveillance

Cisco ISR Overview

This new solution allows video surveillance modules to be plugged in to Cisco routers (watch a nice video of Cisco ISR IP Video solution). Many of Cisco routers allow for different devices to be plugged in to the back of the router. Wireless networking, IP telephony, Ethernet switches and many other devices can be plugged in to the back of the router to add these services. Likewise, you now can add video surveillance to a Cisco router.

Cisco offers 2 types of video surveillance modules: an encoder and an NVR. The encoder lets you use existing analog cameras. The NVR manages and records video from either the encoder module or from third-party IP cameras/encoders. The NVR comes with a 120GB or 160GB hard drive with an ISCI connection for external storage.

You can use the video surveillance models on a select number of their Integrated Services Router (ISR) line which has over 4 million units deployed. The ISR has four series. All of the models in the top series (3800) supports the video surveillance modules and most of the models in the next series (2800) supports these modules. None of the models in the bottom two series (800 and 1800) support the modules.

MSRP pricing for the 16 channel encoder module (EVM-IPVS-16A) is $4,800 (found online for $3,300) while the MSRP for the 16 channel NVR module (NME-VMSS-16) is $10,000 (found online for $7,700). ISCI Storage beyond the 120GB/160GB on board can be purchased separately.

Advantage: Eliminate Security Systems Integrator

By centralizing all video surveillance services within your existing networking infrastructure, you can use you network/IT engineers to manage data, voice and now surveillance video. While I see issues in this (less expertise in camera configuration/optimization, higher hourly costs), this could be attractive to IT centric organizations.

Advantage: Attractive to customers with existing ISR routers that can support these modules

If you have a 2800 or 3800 series router, you can plug in a DVR/NVR solution. So long as you are not using the modules already for IP telephony or other services, you should be able to quickly add in video surveillance. IT departments with available slots should find this attractive.

Advantage: Attractive to customers who are evaluating purchasing new ISR routers

If you are evaluating a new router purchase, you may find it beneficial to upgrade to a higher series so you can have slots available for adding video surveillance. The incremental cost of moving up should not be dramatic and you can deploy video surveillance as a seamless part of your network infrastructure.

Other Cisco Cited Advantages

Cisco cites increased reliability, network performance and security. Examples include eliminating video surveillance server, easier to provide back up power,

easier to apply QoS, lower latency and embedded security infrastructure.

I think these advantages are modest at best. The main issue in video surveillance reliability is hard drives. Cisco does not improve that situation. With the Cisco ISR solution, you would need to deploy iSCI RAID system which is actually more expensive than leading NVR/DVR solutions. As for QoS, most customers operate satisfactorily with existing video surveillance system without QoS for video surveillance. Nevertheless, this requires its own review at a later date. As for the security, it should be increased but it should not be terribly dramatic. NVR/DVRs today are much more secure than the horror cases frequently cited from earlier in the decade. As such, I think a premium should exist but it should be modest.

Disadvantage: Significantly More Expensive than Leading NVR/DVR Platforms

Whether using the Cisco modules for analog or IP cameras, the solution is far more expensive. As a DVR replacement with analog cameras, end user pricing for the Cisco solution will be about $13,000 to $15,000 per 16 cameras – double the cost of top DVR systems. As an NVR replacement with IP cameras, the Cisco solution costs about $10,00 to $13,000, substantially more expensive than even market leaders such as Milestone or Genetec. Here's how the numbers break down:

- Cisco Encoder module: $3,300
- Cisco NVR module: $7,700
- 500Gb to 1 TB iSCI External storage: $2,00 to $3,000
- Opportunity cost for using 1 or 2 slots on ISR: $500 to $1,000

Such a dramatic increase in price is going to be quite hard to justify for any

organization that is doing a careful comparison of the alternatives. The natural question will arise, "Why don't I just set up a stand alone appliance and save $4,000 per store or branch office?"

Disadvantage: Less Flexible / Expandable

One of the key advantages of moving to IP video surveillance is having the freedom of a software only solution. Unfortunately, this solution locks you into Cisco's hardware. Cisco basic NVR module offers only 1 GHz CPU and 512 MB RAM; the premium one only 1.4 GHz and 2GB RAM. This will limit your ability to handle megapixel cameras and analytics. You can, of course, only choose to do analytics at the camera but this is quite constraining and could deny you significant savings from the increase in processing power that other NVR/DVR appliances will be using to do more analytics centrally.

The risk is extremely high that this hardware will block you from taking advantage of some of the critical and most valuable advances in video surveillance that are emerging now and will continue to evolve over the next 5 years. Cisco certainly offers alternative deployment models but this defeats the purpose of placing a module inside your existing router.

Disadvantage: Mediocre Video Management capabilities

As a video management system, Cisco offers no significant features that are not common on any mid-level DVR or NVR. Moreover, they are weak to moderate on analytics, megapixel cameras (less variety), POS / ATM support, access control integration and advanced search – all key elements for today's surveillance state-of-the-art surveillance systems.

Megapixel cameras, 3rd party integration and analytics are driving most customer purchasing at the enterprise level. Customers are essentially going to have to sacrifice some of these benefits to participate in the Cisco solution. Such sacrifice will be hard for many to do.

Disadvantage: Deployable on only a small percentage on routers deployed

While the marketing efforts focus on support for Cisco's ISRs, only a small percentage of ISRs in the market are actually compatible for this solution. None of the very popular 800 series, 1800 series or 2801 routers will work with this solution. Therefore, of the 4 million or so deployed ISRs, a large portion do not support video surveillance. And if you need to support analog cameras, even the 2811 does not support the solution.

The problem, then, is that most people can't even use it even if they wanted to do so.

Disadvantage: Not realistic to deploy new routers simply to add video surveillance

It's unlikely that organizations will purchase new routers simply to take advantage of the video surveillance modules. It's logistically complex to coordinate purchasing routers and video surveillance at the same time. Almost everyone has routers and video surveillance already in place. Timing both at the same time or the video surveillance after the routers will be necessary but challenging.

Conclusion

The Cisco IP video surveillance router plug-ins are a disappointment. With many constraints, few advantages, a much higher price and limited flexibility, these modules will have limited appeal.

Do the benefits of Cisco's networking advantages outweigh its much higher cost and limited video surveillance abilities? I think most will judge "no".

III

Evaluating New Products

Chapter 21: 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 gloss 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 gauge 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 22: 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

Does 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 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 there 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% ot 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 23: 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 a 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 a 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.

Alphabetical Index