Best Practices Guide For
Administration, Policy, And Management
Of Video Surveillance Systems

ABSTRACT

The purpose of this document is to provide companies with guidelines on the overall administration, policies, and management of a video surveillance system and to provide recommendations for best practice implementations for video surveillance environments.

securityhive
The encyclopedia for the security industry

Developed by SecurityHive.com
18134 S.W. 92nd Court
Palmetto Bay, FL 33157
www.SecurityHive.com

Created: April 11th 2011

Updated: October 10th 2013

Table of Contents

THIS PAGE INTENTIONALLY BLANK

1 Legal Disclaimer

This *Video Surveillance Best Practices Guide* (herein "Guide") is made available for educational purposes only as well as to provide general information and a general understanding of industry acceptable implementation concepts and is not designed to provide legal advice. By reading this Guide you understand the information provided is intended to be current and accurate, however, the information presented may not reflect the most current legal developments, regulatory actions, or court decisions. These materials herein may be changed, improved, or updated without notice. SecurityHive is not responsible for any errors or omissions in the content of this Guide or for damages arising from the use or performance of this Guide under any circumstances.

DISCLAIMER: Although this Guide is designed to provide accurate and authoritative information with regard to the subject matter covered, the authors and their organizations accept no responsibility for errors and omissions. THIS GUIDE IS PROVIDED "AS IS." THE LICENSOR, THE COPYRIGHT HOLDER AND THE CONTRIBUTORS TO THIS GUIDE MAKE NO REPRESENTATIONS OR WARRANTIES (i) EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON INFRINGEMENT; (ii) THAT THE CONTENTS OF THIS GUIDE ARE FREE FROM ERROR OR SUITABLE FOR ANY PURPOSE; AND (iii) THAT IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS, OR OTHER RIGHTS. IN NO EVENT WILL THE LICENSOR, THE COPYRIGHT HOLDER, AND THE CONTRIBUTORS TO THIS GUIDE BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES FOR ANY USE OF THIS GUIDE, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR OTHER DATA OF YOUR INFORMATION HANDLING SYSTEM OR OTHERWISE, EVEN IF THE LICENSOR, THE COPYRIGHT HOLDER OR ANY CONTRIBUTORS TO THIS WHITE PAPER IS EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2 Preface

As video surveillance systems become more commonplace, many reports and research organizations have revealed efficient and effective methods used by companies to implement video surveillance solutions and how best to comply with the many requirements of corporate governance, as well as local, state, and federal regulations.

Traditional analog video has been around since the 1920s and that same basic technology is used by most CCTV video surveillance systems today. Just as CDs and DVDs have replaced audiocassettes and VHS tapes, IP-based networking and video storage systems are replacing analog solutions. There are still numerous areas where analog systems perform well and can meet the stated requirements of proper video surveillance. According to research firm In-Stat, IP cameras will surpass analog camera sales in 2014. For new installations, or when replacing older components, a digital IP-based system is quickly becoming the preferred technological choice. This document will cover the best practices of video surveillance implementations.

With advances in computer technologies, video surveillance management systems are converging toward a more digital, IP-based, infrastructure. With IP-based solutions capable of interfacing with recorders, switches, computers, servers and the Internet, implementing stronger overarching management functionality is possible. New technologies and management advances are presenting new concepts that enable organizations to get the best return on investment for their video surveillance solution. These methods are referred to as “best practices.”

“Best Practices” are efficient and effective methods used by companies to comply with requirements and business needs. Following are best practice guidelines for implementing and managing a video surveillance solution.

2.1 SecurityHive Video Surveillance Best Practices Guidelines

- □ Perform a complete site survey to determine fields of view, total surveillance area to record, cable run lengths, camera positioning, and any other requirements-related issues.

- □ Select the fewest number of hardware manufacturers; ideally one per hardware component type such as cameras, monitors, storage devices, etc.

- □ Select the fewest number of models of IP-cameras for best long-term maintenance and management.

- □ Configure and utilize Network Time Protocol (NTP) for an accurate and consistent time source for all video surveillance devices in the network.

- □ Designate video surveillance network traffic with the QoS DSCP value of CS5 and provisioned in either a priority or bandwidth queue on all applicable routers.

- □ Implement access control techniques that limit workstations that can configure and view an IP-camera directly.

- □ Ensure proper lighting conditions for Field of View (FOV) areas as well as day and night and color versus black and white recording requirements.

- □ Determine if audio recording for specific areas is required. Review any applicable laws, statutes, and/or ordinance referring to the recording of audio.

- □ Utilize the best and most affordable lens and iris combination for the specific cameras.

- □ Utilize Megapixel IP-cameras as often as possible to increase the Field of View (FOV) while decreasing the number of physical cameras needed.

- □ Configure cameras to the highest possible quality (in other words, the lowest amount of compression and review the storage best-practices sections for recorded video capacity concerns).

- □ Set camera feeds to full 30 frames per second (fps), highest variable bit rates (VBR), and highest camera resolution (including megapixel) as possible.

- □ Use MPEG4 or H.264 file format. Many IP-cameras can be configured to MPEG4, H.264, and MJPEG codec technology. All have advantages and disadvantages.

- □ Use appropriate Pan/Tilt/Zoom (PTZ) day/night capable cameras when constant recording is required.

- □ Install as many cameras as necessary to cover all relevant FOV areas.

- □ Determine what alarms and event triggers notifications the video surveillance duty manager should receive.

- □ Use PoE network switches for IP-cameras to simplify installation (where possible).

- □ Determine the number of network switches needed for all IP-cameras and storage units.

- □ Consider a dedicated network or subnet for video surveillance dataflow apart from the company's main data network.

- □ Minimize any single point(s) of failure.

- □ Ensure elegant cable runs and optimal cable management techniques.

- □ Use only cameras that are Real Time Streaming Protocol (RTSP) enabled. This protocol provides the most universal support and maintenance. RTSP is the foundation for the ONVIF Specification.

- □ Use a surveillance video management system that provides: i)the best live-viewing capabilities; ii)extended support for diverse storage devices; iii)is highly scalable; iv) provides centralized management; and v)supports analog and IP-cameras (hybrid).

□ Enable surveillance video management software to create low-resolution companion files.

□ Select surveillance video management software with the quickest, easiest-to-use, most relevant search and playback capabilities. (Search should support extensive metadata.)

□ Determine retention policies for each individual camera based upon the uniqueness and importance of the subject matter under surveillance.

□ Retention policies need to consider corporate governance, all applicable tort laws, and local, state, and federal statutes.

□ Determine optimal recording times for individual cameras, allowing for pre- and post-time-slot padding or 24/7 constant recording. Do NOT rely on Record-on-Motion functionality.

□ Determine which individual cameras –if any– require live monitoring of video feeds.

□ Determine which individual cameras –if any– require analytics and which analytical behaviors should be utilized. No more than three behaviors for any one individual camera is recommended.

□ Calculate average daily storage requirement for all enabled recording cameras. (Utilize the SecurityHive.com storage and network bandwidth calculator at: http://www.SecurityHive.com/tools)

□ Determine appropriate external storage type for offline storage management (LTO digital data tape or RDX removable harddisk, for example).

□ Establish appropriate replicate, migrate, or purge rules/policies based upon primary and secondary storage requirements and resources.

□ Enable automatic replicate, migrate, and purge policies of captured video feed data files.

□ Determine the most appropriate export destination for general video segment clip selection. This destination should be made known to management and authorized parties.

□ Enable email or texting of alarm/event notification.

□ Enable proper security setting for corporate management and authorized parties to access Export destination(s).

□ Always use barcodes on LTO digital data tape.

□ When feasible, utilize the highest capacity LTO, IBM 3592, or Oracle T10K-D digital data tape libraries.

3 Introduction

This document discusses needs and best practices for implementing an organizational video surveillance system, focusing on the live-viewing, recording, storage, and overarching management requirements of such a solution, as well as the proper documentation of such a solution through the creation of a video surveillance policy manual.

Also discussed within this document are requirements for corporate video surveillance implementations as well as management needs for organizations that must comply with legal requirements and corporate governance issues.

3.1 Background

The need for transparent processes that are subject to rules governing equipment, installation, and employment and use of the resulting recorded material fall under best practice management. Companies that wish to implement a digital video surveillance solution do so for one of the following major reasons:

- Protecting individuals and property onsite from criminal activities
- Providing increased customer service, site operations efficiency, and/or site safety through knowledge of actual events, including video analytic alert notification
- Providing cost savings via less product loss/shrinkage
- Providing public safety by including video feeds to emergency personnel during a crisis
- Providing an access control system
- Enabling forensic analysis of events to establish facts
- Improving staff and customer peace-of-mind

The first part of every organization's *Video Surveillance Policy Manual* should be an explicit and comprehensive listing of the intended purpose or purposes of the system. Replace the above general bullets, if they apply to your environment, with specific examples of precisely what you expect the system to accomplish or what it should prevent. Although you may not be able to list every possible situation, give as many specific examples as possible, such as “capture the faces of individuals painting graffiti on outside vehicles at night,” or “rapidly determine the nature of any pallets or boxes left on the loading dock after the dock doors are closed each day.” Realize that video surveillance cameras are used for three types of reasons:

- Deterrence
- Real-Time Monitoring
- Forensic Recording

For each stated purpose, it is valuable to indicate which of these three usage modes is likely to be used.

An IP-based network infrastructure for a video surveillance system has the following advantages:

- High reliability
- High system availability
- Multi-vendor best-in-class solution support
- Guaranteed Quality of Service (QoS)

- Secured transmissions
- Secure mobility
- Ease of management
- Reduced operation costs

3.2 Scope of Best Practices

Video surveillance processes should be clearly stated and appropriate tools implemented to ensure compliance. Before deploying a video surveillance system, the organization must first understand the issues facing his installation. These issues may be specific to his installation, or common throughout the industry. Organization should have a full understanding of their environment and challenges before choosing and deploying a video surveillance solution.

Where can the threats/dangers come from? Where are the critical areas and potential security breaches? What risks are staff being confronted with? What, if any, non-technical objectives need to be decided upon and covered before deployment?

An overall security audit should be performed that would identify areas of high-risk or potential failure. For each type of risk or threat, the necessary combination of video surveillance and other security systems (such as intrusion detection) can be determined and then addressed in the design of the surveillance solution.

Best practices deal with various issues that an organization should factor into their decision making process regarding how to best comply with legal requirements, corporate governance issues, and expected video coverage areas of their video surveillance solution. The following sections also provide various "best practices" identified from numerous implementations of video surveillance systems.

4 Video Surveillance Program Policy Statement

Each company should establish a formal policy that defines its *Video Surveillance Program* and require the organization’s governing body to formally adopt the policy. The person who is primarily responsible for implementing and managing the *Video Surveillance Program* usually guides development of the initial draft of the policy and presents it to the governing body for review and approval. It is generally useful to involve top management officials, union officials (if the employees are represented), and local legal counsel in reviews of the draft policy.

To show proof of governing board adoption, some entities include a header on their entire document that contains the policy number, adoption date, and appropriate signature(s). Other common methods include a page documenting meeting minutes or a formal adoption page complete with signature(s).

4.1 Video Surveillance Requirement

Within this section of a document a policy should cover the written statement for covered employees, customers, and other individuals that engage with the organization during the presence of a video surveillance system and the requirements behind the system. Preferably, the organization can introduce video surveillance with the key stakeholders and its community beforehand. It is best to have a majority of stakeholders involved during implementation, allaying their fears, and acknowledging the very real paranoia of video surveillance. **<u>It is critical to get any inherit mistrust under control early and then move ahead with the implantation project.</u>**

Federal common law (Fourth Amendment to the U.S. Constitution) says that video surveillance systems may not intrude on an individual's "expectation of privacy." This includes employees, customers, vendors, visitors, and the public. In general, open public spaces, such as a sidewalk, have a lower expectation of privacy than a smaller, private space, such as a dressing room. However, except for legally approved police covert surveillance, the best strategy is to provide signage informing all individuals that a particular space is “monitored by video surveillance cameras."

State and municipal laws vary, but most jurisdictions explicitly prohibit cameras in bathrooms, locker rooms, changing rooms, medical treatment areas, or any location where people expect complete privacy. Numerous States also have anti video-voyeurism statutes. Video surveillance systems should never be used for any personal purpose, for spying, or for entertainment. Monitoring audio conversations or event out of mere curiosity is not permitted and may be illegal (applicable wire-tapping laws).

Requests for additional areas or regions of interest that should be placed under a video surveillance should be clearly communicated and part of any policy. Any member of an organization should be allowed to submit a request for the installation of equipment to the video surveillance supervisor who will determine the need and requirement for such coverage.

4.2 Surveillance Monitoring

This section of the policy addresses specific issues and reasoning related to the areas under surveillance, items being monitored, and individuals that are being monitored. Company informational materials on prohibited use of captured video or the misappropriation of captured video includes pamphlets, brochures, and company newsletter articles. These materials are often distributed to new employees with orientation materials and are communicated via postings and displays in common areas of the workplace and seminars. Put this information in your employee handbook and require an employee signature.

4.2.1 Continuous Surveillance of an Area

This section of the policy will clearly state the declared area of continuous video monitoring and the responsibilities of those employees, customers, and other individuals being monitored.

4.2.2 Reasonable Suspicion Surveillance

Organizations may want to include examples, in the policy document, of the legally accepted reasons for ordering reasonable suspicion surveillance and use wording that the employees are most likely to understand.

4.2.3 Post-Accident Surveillance

This section of the policy document should explicitly state when the surveillance of covered employees would incur after any accident, or accidents, in order to remove all decision making over whether to initiate separate surveillance of an individual. However, organizations must still decide by which authority to perform the surveillance and must clearly indicate on any accident report(s) which authority they are performing any separate surveillance. The policy may also use a more stringent definition of an accident, for example.

4.3 Surveillance Methodology and Integrity

This section of the policy document describes how system tests are conducted in accordance with stated corporate guidelines, stated corporate governance requirements, or local, state, or federal laws.

4.4 Applicable Personnel

This section of the policy document should list every job that includes direct surveillance duties or duties covered by the surveillance system, regardless of the percentage of the position's duties that are surveillance related. The policy should also state that all employees and their duties have been reviewed for surveillance needs.

Because a significant percentage of all court cases related to video surveillance issues involve chain-of-custody matters, organizations should review all duties and potential duties of each job title and employees involved in the handling of the video surveillance data. Front-line operations and surveillance supervisors usually perform preventative maintenance duties on the video surveillance equipment, so these individuals and their responsibilities should be clearly noted.

Refer to the Legal Review section (5.3) for the determination on which of the organization's applicable personnel is best suited for selecting what video is to be deemed relevant for any particular event of interest.

4.5 Designated Contact Person

This section of the policy document should clearly identify who it is that should be contacted with concerns about the video surveillance activities within an organization. Although there is no requirement that specifies where in the policy to include the identity of the contact person, some employers place this information at the end of the policy document. A Designated Contact Person should always be clearly identified on the premises under surveillance.

The person designated to answer employee, customer, or other individual's questions about the video surveillance program is often the person responsible for the overall program administration. For smaller organizations, this may be a human resources manager, an operations manager, or a general manager. The contact person's position title, work address, and work telephone number should also be included, as well as the words "and their successor."

The contact person is usually the primary individual for reviewing any video of interest and for exporting specific areas of interest from all recorded video and forwarding it on to the organization's governing body, legal counsel, or law enforcement agency.

Refer to the Legal Review section (5.3) on the determination of the organization's applicable personnel best suited for selecting what video is to be deemed relevant for any particular event of interest.

4.6 Refusal Behavior and Consequences

This section of the policy document should provide examples for any employee, customer, or individual with behavior that constitutes a refusal to be subjected to video surveillance monitoring and what recourse, if any, they would have.

5 Education and Training

It is important for any company to discuss and apply best practices for the education and training requirements contained within corporate governance guidelines, as well as any and all local, state, or federal legal requirements, for the proper implementation, use, and handling or a video surveillance system.

Rumors can begin almost immediately when company personnel are informed of a video surveillance implementation. Rumors about covert camera usage can be very damaging. Questions will arise such as, “why are they putting in cameras?” “What are they watching?” “Why do we need so much surveillance?”

“I had done my best to develop a relationship with the employees,” stated the head of security for a large corporation. When the cameras came on the scene, he worried that he was about to take a giant step backwards. Then this security chief had a new idea. As the control center had glass walls, he decided to turn the monitor’s screens around, so they faced outward. With this change, any company employee walking by the control center could see exactly what the cameras are being used to observe. “I told employees, come on down, you can see what we're looking at. We can show you how the system works. We'll let you play with the controls,” the security chief added. “That alone allayed the monitoring fears.”

To many of the employees, the installation of cameras screams of Big Brother. The security chief assured employees that the system was more about customer service (such as letting employees back in the building if they accidentally got locked out during a smoking break), to give employees peace of mind and to keep an eye on more places than was otherwise humanly possible (data centers, for example).

If your policy is strict but the reasoning and motivation is clearly explained (see section 3.2), and if you also demonstrate a certain level of reasonableness in the way you handle surveillance and monitoring matters, employees will have a better chance of understanding and develop their own peace-of-mind.

An illustration occurred of the risks created through covert surveillance in November 2004, when nurses at Good Samaritan Hospital in Los Angeles were in a break room where they detected a beam of light coming from a wall clock. They were shocked to discover a hidden camera with a tiny lens in the face of the clock. The nurses immediately spread the word to their colleagues; eventually they discovered a total of 16 hidden cameras in the clocks of break rooms, a pharmacy, and a fitness center, among others. The fact that the nurses hadn't been informed about the cameras upset them because some of them changed their clothes in the break rooms. They felt that their right to privacy had been violated. A California Nurses Association press release stated, "This is a pervasive problem throughout the hospital that is a disgraceful violation of the legal privacy rights of the RNs and reflects a deplorable attitude of the hospital administration towards its caregivers."

Hospital officials defended their actions claiming they had planned on informing the nurses, that it was standard practice in hospitals, that the cameras were installed for security reasons, and that the cameras hadn't been turned on. They also noted that the nurses' employee handbook, which all must sign, states that surveillance might be used.

Ultimately, the situation could have been avoided if hospital executives had informed the nurses of their plans beforehand, explained that the cameras were for their safety, and made them overt instead of covert. By neglecting to inform the nurses until the cameras had been discovered, the hospital aroused suspicion and ill will. The bottom line on hidden cameras is that there may be a place for them, but you should have your legal team review that need to weigh the risks and use such strategies with due caution.

5.1 Training for Video Surveillance System Employees

Required video surveillance system management training is often incorporated in the employee orientation process. Many employers find it difficult to cover all the required information in a standard classroom setting, particularly if questions, discussions, and role-playing are included. However, a basic understanding of the legal requirements for proper “Chain-of-Custody” handling and local laws is imperative.

An organization with a unionized workforce has additional educational, training, and potential legal issues to comply with. According to the Labor Research Association, any introduction of surveillance into a unionized workplace could be cause for a union grievance. A report titled “Employer Snooping: What Rights Do Workers Really Have?” advises, “When a company seeks to introduce video surveillance it is attempting to change working conditions, according to the NLRB. As a result, the terms of these policies are considered a 'mandatory subject' of collective bargaining and must be negotiated with the workers' union.” The report goes on to cite some examples of what an employer and union might negotiate, including allowing workers to defend themselves against accusations and agreeing that some non-work areas remain camera-free.

Investing is a credentialing program for an employee or a set of employees could be one of the best investments a company could make when it comes to video surveillance. Review some of the societies and credentialing programs listed below and determine which one would be best for your company.

Certified Safety Professional (CSP)
Certification in Homeland Security (CHS)
Emergency Number Professionals (ENP)
Registered Communication Distribution Designers (RCDD)
Certified Technology Specialist (CTS) for audio-visual systems
Crime Prevention Through Environmental Design (CPTED) Specialists
Certified Protection Professional (CPP)
Professional Certified Investigator (PCI)
Physical Security Professional (PSP)

6 Video Surveillance Program Implementation, Administration, and Management

6.1 Management Focus

Historically, video surveillance systems were focused on the number of cameras they could display at any one time. New video surveillance programs are becoming more centralized around video feed recording, event triggers, retention, storage management, search, playback, and export capabilities.

6.2 Management Oversight

Scalable systems will allow the video surveillance system to add cameras over time so that as a company grows, its video surveillance system will grow with it. Over time, companies that are expanding their video surveillance deployments over large areas will look to solutions that can self-associate rather than require manual programming. They will also need an enterprise-class architecture that can scale in order to manage all the cameras, servers, and storage devices necessary to live-view, record, store, playback, and export all camera generated video data.

The organization is ultimately responsible for maintaining a video surveillance program that complies with all local, state, and federal laws and its own corporate governance policies. In the case of Bright versus United Corp. (2008 WL 2971769 V.I. July 22, 2008), the defendant, a supermarket that had an installed video surveillance system, was held negligent in the case, with a focus on the improper training of the frontline managers that were interacting with the video surveillance system.

6.3 Legal Review

6.3.1 Selection of Legal Review Personnel

It is imperative that an organization determine, especially at the initial phases of the implementation of a video surveillance system, which personnel within the organization has the required legal training, background, and expertise needed for determining the legal standings of recorded video feeds.

Again, in Bright v. United Corp., the Supreme Court stated, "… It is certainly not within the discretion of a store manager to determine what portion of the available recorded surveillance footage is relevant to anticipated litigation. . . . To allow store managers unbridled discretion to determine what footage to retain would encourage the destruction of relevant evidence by allowing managers to destroy unfavorable footage under the pretext of routine practice."

The Supreme Court found that the defendant's destruction of the recorded surveillance footage prior to and after the plaintiffs "slip and fall" indicated its "bad faith and fraudulent intent to suppress the truth." It continued, "Given the importance of determining how and when a foreign substance causing a slip and fall originated, it is unlikely that any reasonable business manager would fail to evaluate the portion of the video surveillance preceding the slip and fall. Therefore, this Court finds that the failure of the Plaza's manager to retain the recorded surveillance footage prior to and after Bright's fall ***shocks the conscience of the court and creates a presumption of fraud***" (emphasis added).

The court concluded that the defendant "both intentionally and fraudulently destroyed relevant evidence." It also found that the plaintiff had been severely prejudiced, since the destroyed footage was perhaps the only evidence upon which she could rely to prove that defendant had notice of the spill.

Therefore, the need for the advice and counsel of experienced legal personnel is just as important in the overall implementation of a video surveillance system as the technology itself. In the above case, we see an organization that had put in place a video surveillance system with the goal of protecting their organization and then because of poor legal review, the system became a liability.

Another area of concern from a legal point of view is the use of fake or deactivated cameras. Fake or deactivated cameras attempt to get the deterrence value of video surveillance without incurring the expense of actual video storage and maintenance. Hidden cameras, obviously aim not to stop illicit behavior but to catch it for the record. However, all of these strategies create risks. A manager of safety, security, and asset retention at a large international logistics company thinks fake cameras can impart a false sense of security. For example, if someone is standing in front of what appears to be a camera and another person pulls a gun and takes the first person's wallet, you should be able to search for such an event on recorded video, but you cannot. You then have to tell the person that the camera(s) were fake. **The legal liability from negligent security actually exists in this situation.**

Another expert in a retail loss-prevention consultancy firm also advises caution on the use of fake cameras. One of the things you have to be careful of is whether you have an obligation to provide certain levels of security. **If you don't have cameras and something occurs or you have dummy cameras, you could be liable for negligent security.**

Many lawyers believe there are limited circumstances in which fake cameras are appropriate but that they generally do more harm than good.

Expert legal witnesses, who trial prosecutors engage to testify on the contents of surveillance video, state the importance of "Chain-of-Custody" capabilities for all retained video. Experts state a preference for proper Chain-of-Custody audit trails over that of "watermarks" as a potential watermark could actually impair the area of interest on the video. The minimal requirements for video quality settings that are required to ensure a conviction in a court of law are:

- 640 x 480 resolution (704 × 576 resolution preferred)
- 4CIF (see section 6.1.3)
- 30 FPS

The ability to create low-resolution companion files for typical playback and review allows for the high-resolution original to remain offline until the court needs evidentiary review or court-appointed personnel with associated Chain-of-Custody audit trail documentation.

Best practices demand that all retained video follow proper Chain-of-Custody procedures to avoid video being dismissed as evidence in court. Defense lawyers are able to have video evidence ruled inadmissible anytime the video file itself has been altered or manipulated. Any video management systems (VMS) that reduces or alters image quality after initial capture, just to save on data storage space or for whatever reason, must be avoided.

6.3.2 Proper Operation and Training from The Legal Standpoint

Each organization must have an employee or employees responsible for ensuring the proper operation of a compliant video surveillance system. Large employers often have a separate position for managing the system. More than one employee can perform the responsibilities of this position. Small employers usually do not have a separate position; the system management functions are assigned to an employee or employees to perform in addition to their other duties.

Video surveillance system managers come from various backgrounds and there is no particular discipline that seems to provide a more appropriate experience than any other. The most common backgrounds include general manager, operations management, safety, risk management, human resources, and administrative assistant. The primary requirement is that they are very knowledgeable of regulations, be they corporate governance, local, state, or federal laws.

Whether this position is a full-time position by a dedicated employee or a shared duty responsibility from several employees, industry credentialing such as CSP, CHS, or PSP (for example) should be request or at least encouraged. See Section 4.1 for more information on industry credential programs.

6.4 Internal Administration

Any documented policy should clearly identify and answer various system management issues including the following:

- Who has day-to-day access to the system, and why, and what are their duties?
- What are the rules for managing the day-to-day access, such as issuing passwords, checking log files, and training?
- How is physical security for the system components maintained?
- What is the policy for physical access and who is in charge of the physical access?
- What are the crisis management procedures?
- How is system maintenance handled?
- What is the process for how issues, problems, and complaints are handled?
- How are video “clips” handled?

7 Video Asset Management: Hardware, Software, and Networking Infrastructure

With newer technology and commercial off the shelf (COTS) technology products, video surveillance has become easier than ever to deploy. Video surveillance equipment now supports TCP/IP computer networking protocols increasing the ease and usability of video surveillance solutions. These IP-based devices can communicate over any standards-based computer network. In contrast, analog systems use dedicated point-to-point cabling from the camera to the viewing/recording station.

Modern video surveillance technologies have changed the way businesses manage video. These new technologies integrate video capture, video cataloging, and multi-tiered storage with proven data management methodologies, all while leveraging investment in existing IT infrastructure. The result is a new type of networked video, with fast efficient storage, quick retrieval of specific areas of interest and system scalability that supports even the largest enterprise organizations. Organizations must commit to the upfront planning and consideration regarding how the system will grow in the future in order to receive the most benefit from networked video surveillance solutions.

Certain requirements such as reliability, high availability, resiliency, cost-effectiveness, a high degree of scalability, and the use of best-in-class products are emphasized in utilizing these best practices. An emphasis must be placed on the actual camera(s), lens, and lighting conditions as without a quality input, the rest of the solution is significantly degraded.

With best practice infrastructure guidelines, an organization will:

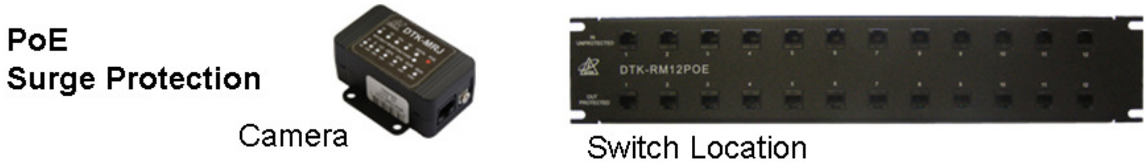
- Procure the best affordable quality equipment
- Capture more useful video data and retain it for longer periods of time at higher quality
- Provide over-arching centralized management of the files, storage, and usability
- Control user access and privileges
- View video either in real-time or through forensic mode through archives and search tools
- Provide sustainable total cost of ownership and effective infrastructure management
- Experience rapid and affordable deployment with massive scalability

IP technology over an Ethernet network infrastructure, combined with digital video, resolves the operational and technological limitations faced in traditional analog CCTV systems. In addition, it is affordable and cost-effective for mass and customized deployments. The concept of video collection and monitoring have also expanded and made possible the delivery of excellent video quality that can be displayed securely and over longer distances.

Proper network configuration and tuning has cost considerations that must be accounted for. Working with static or dynamic IP addresses, VPNs, firewall rules, and other network management tools add to the cost of implementation and, to a degree, on-going maintenance.

7.1 Power and Surge Protection:

An important element of the health and stability of a complete video surveillance infrastructure is a reliable power and surge protection solution. Power over Ethernet (PoE) devices and most digital (IP) equipment devices in general represent a class of systems in which sensitive circuitry must be protected. These systems are extremely vulnerable and need to be properly protected from any potential electrical and storm related power surges. In a typical system, all of the cameras are networked together through. If one camera in the system receives a surge, the surge can flow to all of the other connected components. This includes but not limited to video servers, cameras, Ethernet extenders, and video encoders.



Within a video surveillance solution, the technology focus areas boil down to the input devices (cameras), the output/reviewing devices, the network infrastructure, the video management software, the data recording, and the multi-tiered storage repository for all of the video feeds.

Let's review these six topics:

- Input Devices (i.e., cameras): The cameras can be IP-cameras or analog cameras with the appropriate digital encoding capabilities.
    - Number of desired video channels (cameras) within the organization
    - Number of video streams coming over a single link
- Output or Reviewing Devices (i.e., laptops / desktops computers): These devices have the appropriate client software installed. The clients communicate with the various storage management nodes to facilitate remote monitoring and playback.
- Network Infrastructure: Typical LAN bandwidth of 1000 Mbps to 10 Gbps; Video feeds running over a dedicated network connection; Utilize Multicast streaming.
- Video Management Software: The video management software or suite of software components should offer the following functionality:
    - Remote camera management, recording settings, actual recording, storage settings, video monitoring, data service policies, migration and replication capabilities, online, near-line, and offline media management, and overall surveillance video management.
- Data Recording: The surveillance data should be recorded and stored for future reference and analysis. The organization will need to determine the long-term retention needs of the various video assets and determining if all video is valued the same.
- Multi-tiered Storage: With multi-tiered storage devices, the recording and storage functions can be de-centralized for more efficient management. The storage devices can exist in a different location than the recording and video surveillance equipment, providing greater flexibility and redundancy. The multi-tiered storage also provides the system with very long term retention capabilities not found in typical storage solutions.

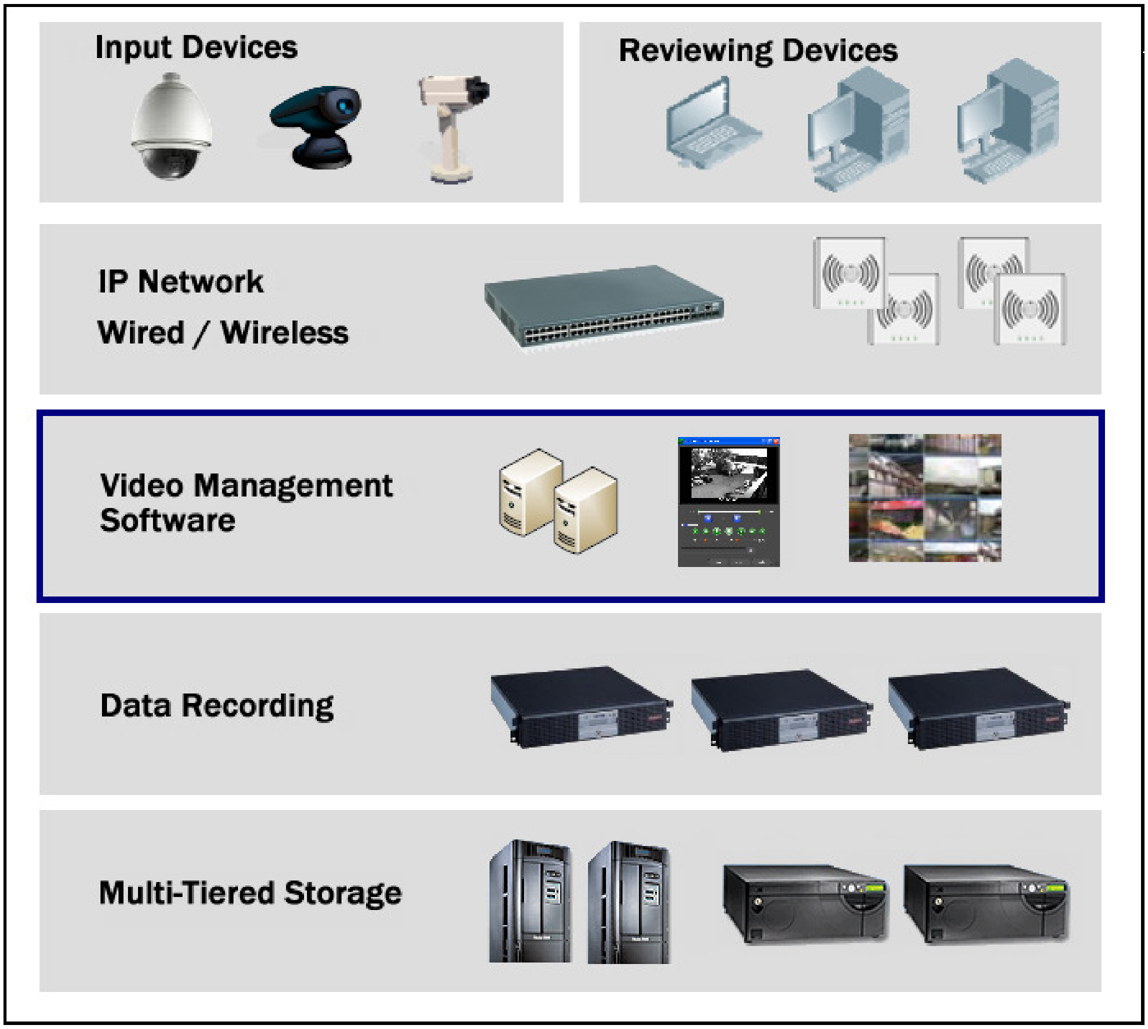


Figure 1: Enterprise IP Surveillance Solution Infrastructure

7.2 Camera Specifications and Requirements

Fixed and mobile camera capture requirements should also be dealt with and accommodated. Basic best practices leverage the fact that cameras love light and thieves hate light. Add lighting wherever possible. The location of the camera and the correct lens are keys to quality video capture and the overall Field of View (FOV).

Items to consider for ideal coverage and best results:

- Camera specifications and requirements
    - How many cameras are required?
    - What are the "areas of interest" for recording requirements?
    - What are the key FOVs?

- Collection Procedures
    - Determine the best lighting conditions of each camera location.
    - Determine where de-centralized video monitoring is needed.
    - Determine what metadata information should be assigned to each video feed.
    - Take a photo of the place where you plan to mount the camera. Mark the exact spot on the photo.
    - Take a photo with the flash OFF of the approximate FOV of the camera.
    - Prepare a map of the facility and mark the location of each camera on the map.

This preparation will ensure that your objectives (Section 3) are met and minimize re-work and setup modifications after installation.

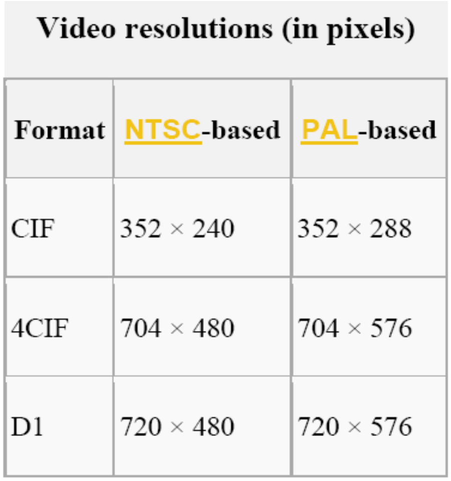
As in any marketplace, there are numerous terms and jargon phrases associated with video surveillance solutions. We will discuss some of those here and explain how they are used. This list is by no means definitive nor complete. See http://www.securityhive.com/glossary/ for more information and definitions for industry jargon/terms.

7.2.1 IP-Cameras

IP-cameras normally generate MPEG, MJPEG, or H.264 images or video streams. Some cameras have the ability to generate various format streams simultaneously. These streams are made available to other devices on the network through a standard IP network interface (i.e. RJ-45 port). Almost all major IP-camera manufacturers support the RTP/RTSP standard protocol that enables easy interconnectivity between network devices and management software. Conventional analog cameras can also be connected to the network through small, adjacent video encoders to digitize the analog images to digital streams. Today’s best practices call for the focus on H.264 or MPEG4 video streams.

7.2.2 Resolution

The term “resolution” is often used as a pixel count in digital imaging. But when the pixel counts are referred to as resolution, the convention is to describe the pixel resolution with the set of two positive integer numbers, where the first number is the number of pixel columns (width) and the second is the number of pixel rows (height), for example as 640 by 480. Another popular convention is to cite resolution as the total number of pixels in the image, typically given as number of megapixels, which can be calculated by multiplying pixel columns by pixel rows. Other conventions include describing pixels per length unit or pixels per area unit, such as pixels per inch or per square inch or pixels per foot.



Video resolutions (in pixels)

Format	NTSC-based	PAL-based
CIF	352 × 240	352 × 288
4CIF	704 × 480	704 × 576
D1	720 × 480	720 × 576

7.2.3 CIF, 2CIF, 4CIF or D1:

Common Intermediate Format (CIF) is used to standardize the horizontal and vertical resolutions in pixels of YCbCr sequences in video signals. A CIF is commonly defined as one-quarter of the 'full' resolution of the video system it is intended for (listed above as 4CIF). Note that this full resolution does not match what is currently referred to as D1 video (based upon Sony's D1 format). Visit SecurityHive.com/tools to use the storage calculator and see the various resolutions sizes.

7.2.4 Lux

Lux is the metric unit for measuring the amount of light that falls on an object and is the equivalent of the British “foot-candle” or “lumen.” There are some differences in the three units of measurement but they are essentially measuring the same thing. The rating could refer to black-and-white images and the quality could be very grainy. The Electronic Industries Association (EIA) has introduced a new standard (EIA-639) that provides consistency between various manufacturers’ specifications of Lux rating. Such a measurement would be listed as “EIA-639 Lux Rating” in a manufacturer’s specifications.

Lux Measurement	Abbreviation	Example
0.001 lux	1 mlx	Starlight on a clear, moonless night
0.25 lux	250 mlx	Full moon on a clear night
3 lux	3 lx	Dark limit of civil twilight under a clear sky
50 lux	50 lx	A residential living room at night with soft interior lighting
80 lux	80 lx	Lighting in a residential or commercial bathroom
400 lux	4 hlx	A brightly lit office area
32000 lux	32 klx	Sunlight on a clear day

7.2.5 CCD / CMOS Imagers

The Charge Coupled Device (CCD) is the component inside the camera that captures the image and converts it into a data stream. Light passes through the camera’s lens and strikes the CCD. Consequently, the image produced by the CCD depends on the quality and setup of the camera’s lens. Camera specifications list the (imperial fraction) diameter of the CCD. Most surveillance cameras fall between 1/4" and 1". For most security systems a CCD size of between 1/4" and 1/3" will provide excellent results. A larger CCD does not necessarily result in a higher quality image; it simply means the camera can gather more light in dimly lit situations.

The CMOS sensor is an active-pixel sensor consisting of an integrated circuit containing an array of pixel sensors with each pixel containing a photo-detector and an active amplifier. There are many types of active pixel sensors most commonly used in cell phone cameras, web cameras, and in some DSLRs. Such an image sensor is produced by a CMOS process (and is hence also known as a CMOS sensor) and has emerged as an alternative to charge-coupled device (CCD) image sensors.

7.2.5.1 Video Compression

Video compression refers to reducing the quantity of data used to represent digital video images, and is a combination of spatial image compression and temporal motion compensation. Compressed video can effectively reduce the bandwidth required to transmit video. Most video compression is **lossy** —it operates on the premise that much of the data present before compression is not necessary for achieving good perceptual quality. For example, DVDs use a video coding standard called MPEG-2 that can compress around two hours of video data by 15 to 30 times, while still producing a picture quality that is generally considered high-quality for standard-definition video.

Video compression is a tradeoff between disk space, video quality, and the cost of hardware required to decompress the video in a reasonable time. However, if the video is over-compressed in a lossy manner, visible (and sometimes distracting) artifacts can appear. Some forms of data compression are **lossless**. This means that when the data is decompressed, the result is a bit-for-bit perfect match with the original. While lossless compression of video is possible, it is rarely used as lossy compression results in far higher compression ratios at an acceptable level of quality.

MJPEG

MJPEG (Motion JPEG) is one of the oldest codecs still in use. MJPEG is usually found in the least expensive cameras. While capable of providing decent image quality, MJPEG is inefficient, resource intensive, and requires massive amounts of storage space. It is bandwidth intensive, which impedes network transmission.

MPEG-2

MPEG-2 is a very common codec and has been in widespread use for more then a decade. It has a good reputation as a stable codec and, up until a few years ago, was the choice of most broadcast professionals. While smaller in file size then MJPEG it is still larger and more difficult to transmit across networks then newer codecs. MPEG-2 dates back to the mid 1990s.

MPEG-4

MPEG-4 (Part 2) is an object-based compression. In MPEG-4, individual objects–rather than a scene of objects–are tracked separately and compressed together to create a data packet. This results in more efficient compression than MPEG-2 or MJPEG and it is scalable, from low bit rates to very high. MPEG-4 is approximately twice as efficient as MPEG-2. MPEG-4 dates back to the late 1990s.

H.264

H.264/MPEG-4 Part 10 AVC (Advanced Video Coding) is a standard for video compression. H.264/AVC is the latest block-oriented motion-compensation-based codec standard developed by the ITU-T Video Coding Experts Group (VCEG) together with the ISO/IEC Moving Picture Experts Group (MPEG), and it was the product of a partnership effort known as the Joint Video Team (JVT).

Most recently H.264/AVC has emerged as the leading codec for commercial video compression. Offering still significantly greater compression than its predecessors, H.264 provides up to 25% better compression then the current MPEG-4 ASP (Active Simple Profile). It also has the best image quality, smallest packet size, provides DVD-quality video and transmits video more efficiently over networks than any of the previous technologies. Unlike the previous codecs, it is able to negotiate rapid complex images and provide razor sharp quality. H.264/AVC is the first of what are known as a complex codecs.

H.264/AVC is the standard for HDTV and runs everything from mobile phones, to PlayStations, to QuickTime and has a large adoption base. In older systems, much was done to reduce frame size, resolution, or other video attributes in order to reduce the amount of storage needed to save the video feeds.

H.264/AVC uses what is known as a Variable Bit-Rate (VBR). VBR allows a codec to change its bit-rate dynamically to adapt to the “difficulty" of the audio and video being encoded. In the example of a swinging PTZ or other rapid movement, a higher bit-rate to achieve good quality is required, while less active scenes can be coded adequately with fewer bits. For this reason, VBR can achieve lower bit-rate for the same quality or a better quality for a certain bit-rate. Older codecs use a Constant Bit-Rate (CBR). Therefore, there are no efficiencies regardless of the scene activity; the bit-rate is constant to whatever it has been set to in the firmware.
Best practice measures push for IP-cameras to record at full 30 frames per second (fps) with a minimal resolution frame size of 720 x 480 or 4CIFs and a VBR. Legal experts state that 360x240 resolution is too low for prosecution of criminal activities seeking possible conviction. The irony of today’s technology is that the IP-cameras have the features and functionality to provide megapixel resolution and high frame rates, however it is the storage requirements that begin to push down this usability to lesser quality video feeds. With sound multi-tiered storage practices (see **Multi-Tiered Data Storage** practices below) in place, an organization can and should strive for the highest possible camera resolution and the highest possible frame rate video feeds.

The bandwidth and capacity required for each camera are calculated upfront, and fixed storage and server capacity are purchased to match the load. This can become a lengthy process since each camera’s resolution, frame rate, compression and motion detection settings must be individually calculated. This fixed architecture is replicated as many times as the camera load requires, which can lead to chronic “over-provisioning” of storage that may never be used.

Swapping in higher-resolution cameras to make a customer happy or beefing up frame rates to meet real-world needs can play havoc with carefully calculated server and storage requirements.

The number of frames per second has nothing to do with the "image quality." While 30 frames per second is real time in NTSC, it is made up of 30 individual snapshots. So while a video recorded at 5 frames-per-second has 1/6th the number of images, it does not have 1/6th the quality; it merely has fewer snapshots (that is of course if everything else is equal—such as bit rate, resolution, etc.) Remember, video is nothing but a succession of still images.

7.2.6 Indoor Dome Camera

The indoor dome camera is used in 90% of general indoor applications. It comes in a variety of configurations, including standard color, day/night, and infrared versions. It can be mounted on a horizontal or vertical surface but is typically ceiling mounted. Lens options on dome camera may restrict their use in certain applications, such as those requiring more than a 20mm video lens.

7.2.7 Box Camera

A box camera is a standard camera that can be mounted alone or in an enclosure. The box camera uses a separate lens that screws on to the front surface and provides flexibility for different FOV requirements and is sold without a lens. An auto-iris lens will have a small cable that connects to the camera for iris control in various lighting conditions.

7.2.8 Outdoor Dome Cameras

Outdoor Dome Cameras are typically hard shell vandal-proof casings that offer the same versatility in a variety of lens options. Day/night outdoor dome cameras are common in applications that have entry and exit points with limited lighting.

7.2.9 Day/Night Camera

The day/night camera is the best choice for low-light conditions. The cameras are standard color during daylight conditions. The day/night camera can switch either digitally of mechanically to a low-lux B/W mode.

7.2.10 Infrared Camera

During no-light conditions, infrared cameras provide infrared illumination of the FOV allowing monitoring of areas with no light available. The IR LEDs are automatically illuminated and the camera switched to the b/w low-lux mode offering camera views in total darkness.

7.2.11 PTZ Camera

Pan-Tilt-Zoom (PTZ) cameras offer the ability to view in all directions and optically zoom in as required. PTZ cameras also include standard color, day/night modes, and a few IR PTZ cameras have been introduced recently. PTZ cameras can be pointed in any direction by an operator and can be optically zoomed in on a specific object. Automated "presets" can be set into the camera that moves the camera from one area to another area for a determined amount of time. Options include auto-tracking applications that dynamically track objects in defined areas.

7.3 Output or Reviewing Devices

There are three primary methods for reviewing or displaying the content of a video surveillance solution. By either using a laptop, a desktop, or a mobile device, you should be able to search the stored video assets, select the most relevant asset(s) to review, and then display them on the monitor or display of the laptop, desktop, or mobile device.

Refer to section 5.3 for the proper administration of reviewing of any and all recorded video.

7.4 Network Bandwidth

Contrary to misconceptions, there is typically enough available bandwidth in a modern LAN infrastructure to support video surveillance solutions. For the past decade, organizations have deployed switched (point-to-point) 100-Mbps links to user desktops and other edge-connected devices. The effective throughput of each link is approximately 80 Mbps. Given these throughput ratios, a single LAN-edge link can support 40, 2-Mbps video surveillance streams. Many enterprises and some other organizations have been purchasing switches that support 1000 Mbps or 1 Gigabit to the desktop for several years, given "Gigabit per port" prices have approached 100-Mbps price per port. In these cases, with overhead, the throughput of a single 1000-Mbps link would support 400, 2-Mbps video streams.

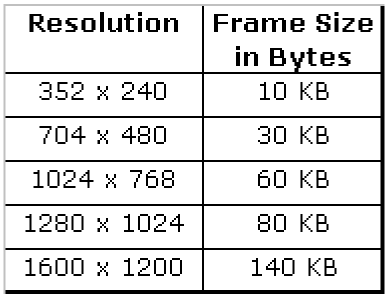
Best practices suggest that video surveillance deployments carry less than one hundred video streams when aggregated across network switches, as the video traffic traverses the core of the network where multiple Gigabit or 10-Gigabit links would be deployed. Thus, it is unlikely that video surveillance would put a strain on a typical organization's LAN.

A video file is a collection of data. File size refers to how much video data is contained in this single unit of measure. The larger the file size, the more bandwidth (the amount of data that can be transmitted in a fixed amount of time) and computer resources are required to display, record, and transfer a file. The overall size of a file of video data can be affected by image frame size (resolution), bit-rate, amount of motion, compression, and various other factors. Ultimately, this can affect the amount of video recording you will be able to store and the overall performance when viewing and recording multiple cameras simultaneously.

A simplified network bandwidth equation is as follows:

Bandwidth = Resolution x Frame Rate (fps) x Number of Cameras.

Use the following estimates of frame size in bytes based on the resolution of the camera:



Resolution	Frame Size in Bytes
352 x 240	10 KB
704 x 480	30 KB
1024 x 768	60 KB
1280 x 1024	80 KB
1600 x 1200	140 KB

(See the SecurityHive.com/tools for the storage and network bandwidth calculator)

If a camera is set at a resolution of 704 x 480 (4CIF), it will have a frame size of about 30 KB (according to the chart above). Convert this to bits to calculate the serial bit rate. There are 8 bits in a Byte, add network overhead and use 10 bits/Byte. Thus, 30Kbytes equals 300Kbits.

Network bandwidth is directly related to the frames per second (fps). If the frame rate is set for 1 frame/sec, the bandwidth or data rate generated is 300Kbits/sec. If we set the camera to deliver 30 frames/sec, the data rate is 9000K bits/sec or 9Mbits/sec. If we have 10 cameras running at this frame rate, the bandwidth is (x 10) 90Mbits/sec. On a typical 100Mbits/sec network (commonly referred to as a 10/100 network) you will begin to saturate the network with 10 cameras. Best practices suggest implementing a video surveillance system on newer gigabit networks thus expanding the number of cameras significantly. 10Gig networks are also becoming more viable, especially for 10-megapixel and above IP-cameras.

From a legal prosecutorial standpoint, video frame rates are very important. If you are not looking at full motion video (30fps), you have to ask what happened in between those frames? If you are recording in full motion video there is no room for hypothetical analysis by defense lawyers. Furthermore, a more detailed picture can make it easier to identify sleight-of hand movements. Older technologies have trouble with slow motion and smooth playback under lower frame-rate conditions and higher frame rates tend to compensate for some of the shortfalls of older technologies.

However, even with all of the technological advancements, best practices still recommend that video surveillance traffic be placed on its own dedicated network or subnet infrastructure when available. Adding additional network switches can isolate the cameras and the computers used to store the video from the rest of an organization's network. So, instead of placing the cameras on your main network, you can use a network switch to isolate the cameras from the rest of the network. Place the PC running the IP video management software (see section 6.4 below) on this same network. The video server will allow you to view a small subset of the cameras at one time and notify you of any alarm conditions from any of the other cameras. This reduces the bandwidth on your organization's network.

7.4.1 Network Quality of Service

Video streams and control traffic should be delivered in real-time and cannot be allowed to suffer bandwidth spikes or other unpredictable network behavior. Minimizing surveillance service interruption means that certain rules should be configured on the network traffic to get the highest/strict treatment with low-latency from all cameras towards the recording stations and archiving/logging servers. Video traffic consumes bandwidth and how many cameras an organization has in its network must be considered. The higher the resolution required, the higher the bandwidth that will be consumed by each camera. The bandwidth can vary from a few hundreds Kbps to 3-4 Mbps and higher. This size of bandwidth should be multiplied for each camera and be calculated for the overall number of cameras in the network. Network bandwidth should have 20-30% bandwidth margin to enjoy optimized resources and network overhead that includes all concurrent video streams.

7.4.2 Wireless Technology for Fixed Video Surveillance

Flexibility is one of the strong suits of wireless broadband technology. There are number of wireless network infrastructures that can be efficiently connected with fixed Point-to-Point (PTP), Point-to-Multipoint (PMP) or Mesh wireless broadband infrastructure.

The advantages of high-speed wireless solutions are excellent in both performance and cost-effectiveness. Wireless video surveillance networks eliminate the difficulty of having camera placement dictated by wire or cable accessibility. With wireless, network administrators can place video cameras precisely where they are required. They can also reduce the cost of running cable. Wireless connectivity also enables reliable, cost effective and quick deployment of an organization’s networks. Wireless equipment can be pooled to provide the most cost effective connectivity to meet the requirements of camera placement and actionable, real-time video transmission.

Remote visual surveillance of mission-critical technology and capital assets, such as auxiliary facilities, extended pipelines and storage areas becomes a daunting infrastructure challenge. Transmission of video and other data to provide actionable information and enable faster response times are being more important.

While many organizations have deployed wire based solutions, systems integrators and network operators are increasingly choosing the very real business advantages of using a wireless infrastructure to extend coverage for existing video surveillance networks or establish video coverage at new locations.

Where existing analog Closed Circuit Television (CCTV) networks are deployed, operators can easily add wireless IP-based systems to augment the capabilities. There is no need to incur the cost and time of replacing these installations. IP-based systems can complement the existing network via video encoders.

Many organizations have already deployed wire-based solutions. New video surveillance system deployments or existing ones always need to consider the inherent issues in building out a wired infrastructure. Many others are in the planning stages of deploying new networks and are exploring the selection of wireless networking infrastructures.

The considerations for installing wireless IP-cameras include distance, environment, and interference. Ensure an optimum wireless channel is selected to avert any interference. Keep the unit as cool as possible and avoid any weather conditions that could damage the unit.

With the variations and advancements of wireless networking technology, an organization needs to research and identify the best wireless networking products, including wireless IP-cameras that are available.

7.5 Video Management Software

Video Management Software (VMS) products record video stream data from networked cameras and encoders and route that video data to the appropriate storage resource and video playback monitors. They also provide camera and user administration. The products display live video in graphical user interfaces (GUIs), provide various camera control functions such as pan/tilt/zoom (PTZ) and enable searching for recorded video. Product differentiators include scalability, network management, fault tolerance, operating system, client software support, and the use of standard conventions and protocols

The best product selection will depend on your system requirements and your budget. The three major applications for the VMS software are a) real-time video monitoring; b) recording and storing video; and c) automated notification of alarm conditions. Keep the following questions in mind as you compare video management system products:

- Live Monitoring and/or Forensic Reviewing
- Camera Management
- Camera Quantity Capabilities
- Number of Concurrent Users
- Video Search, Playback, and Investigation
- Recording and Redundancy Options
- Multi-Tiered Storage Management
- Scalability
- Overarching Video Storage Management
- Cost and Licensing Structure

Historically, VMS systems were strictly live video monitoring solutions geared around the number of cameras being displayed in a matrix. These systems would have specific camera controls and usually had organization personnel continually manning the monitoring stations, ready to engage in a situation as it happened.

Today, more and more video surveillance systems are becoming forensics-based, wherein video feeds are recorded, stored away for retrieval, and managed for long-term access, search, and playback. Thus, VMS systems have begun to migrate from a monitoring-based system to monitoring **and** forensics-based solutions that allow users of the system to quickly and easily search and playback previously recorded and stored video feeds for analysis and disposition.

Examples of the video management system (VMS) solutions currently on the market include Milestone™, OnSSI™, Exacq™, Genetec™, and many more. These VMS solutions represent the more well known 'monitoring' side of video surveillance. Visit http://www.securityhive.com/business-directory/ for a more detailed list of VMS manufacturers.

7.5.1 Investigation

The ability to investigate an incident and find relevant video clips is an important consideration for selecting a VMS. Most platforms offer single camera playback, multi-camera playback, and searching functions. Basic VMS systems provide camera playback that allows the user to chose a camera, the time and date, and then select from a list of video assets that fit that criteria. The user may be able to filter events by recording type (show only motion recordings). Playback controls should include play, stop, fast-forward, rewind, and frame-by-frame advance and reverse.

More sophisticated systems allow metadata and bookmark searching capabilities such as camera groups, storage pools, camera locations, camera views, and other user configurable criteria such as officer’s name, case number, or investigator. This metadata capability provides greater access to the stored video assets and provides for more relevant search results.

7.5.2 Exporting Video

Exported files are typically available in a standard format. The advantage of the common format (such as .AVI or .MOV) is that the file can be played in a widely available and free media player, like VLC or QuickTime. Almost all VMS systems export video with a ‘watermark.’ The ‘watermark’ is actually the result of an image or identification number on the video that allows for verification that the video has not been tampered with. This provides for verifiable Chain-of-Custody capabilities, which are also becoming more commonplace when dealing with video surveillance systems.

For legal evidentiary purposes, best practices dictate that all exported video be a verifiable duplicate (legal term: forensic copy) of the originally recorded video and that absolutely no modifications or alterations (as in compression or manipulation) have occurred.

7.5.3 Video Handling and Security

It is very important that every video or still image exported, removed, or archived out of the system is faithfully documented. Every image should have an audit trail or "chain-of-custody" log, including dated and timed signatures of each individual who handles a copy of an image.

For many organizations, a copy of an image should not leave the perimeter of the facility without the signature of the most senior site manager. The room where the video assets are stored should have a locked door, which stays locked and closed unless an authorized individual is going through it. The logging system should include a signature and the date and time of each person who accesses to the system.

The logging system should include an entry for all actions that use or manipulate the system. Changing camera positions, changing operating parameters, and reviewing stored video, are all actions that should be logged.

All requests to view or copy video images from outside the organization’s administrator chain-of-command should be made in writing on a form designed for this purpose, to the organization’s administrator, who should approve the request with a signature and assign someone in his chain of command to implement the request.

Many organizations should undertake a quarterly audit of all logs. Like any good audit, the auditor should not be in the chain of command of the system administrator. For example, the CFO may be a good choice to perform an audit if he is not part of the video surveillance team.

If a legal dispute goes to court, a legal expert being able to substantiate the architecture and workflow of the VMS system may be required to have any recorded video submitted as evidence.

The purpose of the audit is to determine:

- Are the written procedures being followed?
- Are all logbooks and log files current, complete, and accurate?

The written audit report should be provided directly to the senior site manager.

7.5.4 Video Analysis/Analytics

Video analytic systems are increasing intelligent video surveillance without depending on the attention span of security guards. This technology can analyze intelligent video surveillance content intelligently and open up previously hard to find content within video surveillance assets.

Video Analytics is a new and growing technology. Forensic video analysis is the scientific examination, comparison, and/or evaluation of video surveillance feeds that can significantly improve an organization's situational awareness.

Intelligent video analytics software turns video data into information. This functionality automatically tracks and identifies objects, analyzes motion, and extracts video intelligence from analog or digital video streams. It can output analysis and video data mining as real-time events or store this information into an enabled video management system.

Analytics technology has greatly reduced the need to “monitor” video in the traditional sense. Analytic systems capture and deliver user-defined events via email notification, cell phone notification, or panel alerts.

The practical uses for this data extracted from video feeds are virtually limitless from real-time electronic notifications about perimeter breaches to determining department store shopping patterns, detecting vehicle security gate runners (tail-gaters) at secure entryways, measuring traffic density in tunnels, triggering alarms on stolen equipment, to saving energy in unused building space.

Enhancing a digital video management system with analytics enables an organization to cost-efficiently and proactively monitor large video surveillance installations. Rather than relying on the operator to look at the right camera view precisely when an event is occurring, an analytics-enabled system can deliver the event—or a series of events—in progress for assessment and action.

Visual, audible, and messaged alerts can bring potential threats to the attention of the appropriate personnel very quickly. An assessment of the situation and the type of response needed can be initiated accordingly. Digital files of the alerts may be displayed and then stored for future search and retrieval. A quality video analytics solution, like any effective security technology, enables an organization to focus on safe and secure environment, while keeping costs under control.

When evaluating video analytics solutions, an organization should carefully consider the following:

- Monitoring of Video Collection and Analysis Operations
- Selection of Video Segments (or “clips”) for Analysis

Best-in-class analytics systems should integrate easily into an Internet Protocol (IP) network, working with both analog and IP cameras as needed. The system should also easily accommodate the addition of cameras to the network. They incorporate powerful search functionality as part of the analytics package. While real-time crime interdiction is the goal, at times it may be necessary to review video to identify suspects, suspicious activities, or behavioral patterns. Efficient searching allows operators to search for and retrieve specific incidents within minutes.

Due to overall system implementation cost, users sometimes limit analytics to a small number of the cameras in their systems. While this approach seems reasonable from a budget perspective, it fails to increase safety and security. Who can predict exactly when and where the next security breach will occur? Limiting analytics to a few select cameras assumes a level of predictability that does not exist. The more efficient the analytics software in terms of processing capability, the lower the cost of analytics will tend to be per camera, particularly over the longer term as the system expands to meet changing requirements.

A site assessment is critical in order to maximize the success of implementing a video analytics solution to a particular organization. Details such as camera angles, lighting, and video quality that can determine the success or failure of an installation can generally be uncovered and addressed during the site assessment.

If video analytics technology is implemented the right way the first time, the possibilities for successful crime interdiction, risk management, and enhanced operational effectiveness are endless.

7.6 Recording and Storing Full Motion Quality Video

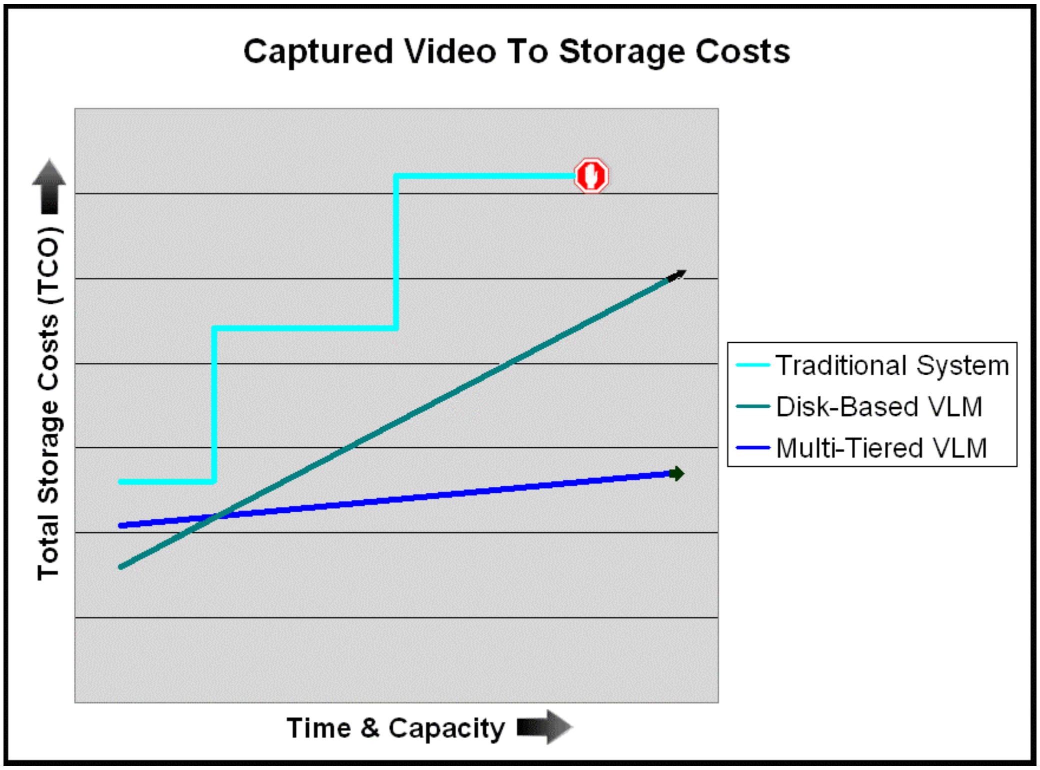
Research performed by Frost & Sullivan in 2008 revealed that over 40 million terabytes of video surveillance storage will be utilized in the United States over the next five years. Research by MarketsAndMarkets.com states that in 2013 over **410 petabytes** of video surveillance data is generated worldwide ***everyday***. And that number will just about double to almost 800 petabytes worldwide daily. In addition, storage will represents 55 to 75 percent of the overall acquisition and operational budget for an average high resolution/high retention video surveillance installation, with the variables depending on the number and type of cameras, frame rates, and the weeks/months of video retention needed. Therefore, best practice measures are surely needed when it comes to the recording and storing of video surveillance.

7.6.1 Video Lifecycle Management

Information Lifecycle Management (ILM) comprises the policies, processes, practices, and tools used to align the business value of information with the most appropriate and cost effective technology infrastructure from the time information is conceived through its final disposition. Information is aligned with business processes through management policies and service levels associated with applications, metadata, information, and data

ILM methodologies have been solving data retention challenges for over three decades. The Hollywood film industry, however, learned that ILM systems are unable to provide the overall management they need because these traditional I.T. storage solutions are not "video aware." Although highly evolved, ILM and traditional means of searching for typical corporate data simply do not work for the now-common video-centric world of the film industry.

Video Lifecycle Management (VLM) solutions have been designed to deal with the specific challenges of storing, managing, and searching video (especially higher image resolution video) in a multi-tiered storage environment. Low resolution companion files and thumbnails used for fast searching–regardless of where in the storage hierarchy the video lives–along with lossless storage are key features of well architected VLM systems. Just like the Hollywood film industry, the surveillance market is now embracing the advantages of VLM.



In a traditional video surveillance system storage, maintenance, and management costs grow until it becomes impractical and too expensive to add additional storage, resulting in the "7-day loop" syndrome. In a comprehensive multi-tiered VLM solution, utilizing online, near-line, and offline storage media an affordable TCO with long-tern retention becomes practical.

Providing the proper overarching file management and handling capabilities for controlling an organization's surveillance storage investment from initial video capture to the eventual purging of the video data file(s) (birth-to-death video file management) is at the center of a comprehensive VLM system. The ability to automate video file migration, replication, and eventual purging practices significantly reduces overall storage costs and routinely frees up initial video capture storage resources.

Best practice video storage requires a heterogeneous collection of storage resources that are best suited to accommodate the long-term needs of the video being preserved. This infrastructure is an active, tiered, storage environment where video is stored and managed based on its value. As video is captured, metadata should be associated and cataloged as to be used within search queries providing more relevant search results.

Best practice guides are especially important for the application of a digital fingerprint being assigned to each video file as it enters the system so that a proper "chain-of-custody" can be delivered as the video asset is moved around a multi-tiered storage infrastructure.

7.6.2 Scheduling

Organizations need to establish the schedule dates and times to meet the needs of their video surveillance policy, as outlined in Section 2, so that it will:

- Enhance the safety and well-being of customers, employees, and the community
- Protect the organization's property and equipment against theft or vandalism
- Aid in identifying intruders and persons breaking the law

In some cases, it may *not* be necessary to record video surveillance feeds 24-hours a day, 7-days a week. In other cases, 24/7 recording may be required. Obviously, the recording schedule has a direct impact on storage requirements and will mandate the appropriate rules and polices to best manage the video data storage resources.

7.6.3 Recording Options: Rules and Policies

Advancing technology has prompted renewed best practices in dealing with overarching recording options for cameras within an organization's video surveillance system. The ability to retain full-motion, 30fps, highest resolution video feeds creates the necessity to properly plan out long-term retention policies for an organization's video surveillance solution. By incorporating specific online, near-line, and offline storage rules and policies, an organization can create an affordable infrastructure that will allow it to keep months and years of video feeds under management and available for fast and easy playback and export.

Video file migration and replication rules and policies need to take into account the organization's available storage resources, such as NAS, DAS, SAN, Blu-ray, RDX, and digital computer data tape, (such as LTO, IBM-TS, or Oracle T10K). Best practices dictate a mix of online, near-line, and offline storage resources for optimal long-term retention periods and best utilization of those storage resources.

7.6.4 Video Storage Policy Example

An example of a multi-tiered storage infrastructure using best practice video retention rules and policies could include the following:

- Begin recording the video feed from camera #8 at 5:00PM (1700 on the 24-hour clock) and end recording at 9:00AM (0900 on the 24-hour clock) Monday through Sunday.
- Initially store this video asset on the network NAS storage device.
- Create a low-resolution companion file upon initial storing of the video feed to the NAS storage device.
- After 72-hours, replicate (copy) that video asset to a LTO digital computer data tape for long-term retention.
- After 30-days, purge the original high-resolution video asset that was stored on the network NAS storage device (keeping the low-resolution companion file on the NAS unit).
- After 3-months, export the digital computer data tape from the tape library device and store on a storage shelving system for easy identification, retrieval, and re-insertion.
- After 3-years, begin rotating the computer data tapes from shelf storage by purging those previously stored video assets and reusing the data tape for new video feed capture, starting with the oldest video computer data tape.

This long-term retention scenario highlights best practices for the video retention of the captured video surveillance from initial capture through final storage. Even when this particular video asset has been stored offline on digital computer data tape, it must remain under the full management of the VMS software solution in order to allow users to quickly search and playback the high-resolution original file without any additional “re-importing” or trans-coding steps.

The availability of low-resolution companion files makes it easy for the end-user to quickly search, identify, and playback the needed video asset without needing to reload multiple computer digital data tapes beforehand.

7.6.5 Retention Times

Much attention has been directed toward dealing with a video surveillance storage requirements and retention times. As stated earlier, this has historically been a matter of the actual pre-set capacity of the primary storage device for all incoming captured video feeds.

Updated best practices dictate video surveillance systems and solutions provide for retention times in terms of years and years instead of days and months. With local, state, and federal regulations (such as tort laws) as well as corporate governance issues, the necessity of very long-term retention of all video assets, at high frame rate, and high resolution is more of a requirement than ever before. In fact, it may be in an organization’s best interest to retain all video assets indefinitely. With the integration of hard-disk based storage resources coupled with computer digital data tape based storage resources (such as LTO IBM-TS, Oracle T10K), these retention requirements can be affordably met with proper video asset management software providing the over-arching management to easily search and playback all video data files, no matter their storage location.

7.7 Multi-Tiered Data Storage

Frost & Sullivan also state that servers and storage infrastructure make up a substantial amount of video surveillance installation costs. There are many discussions about network video recorders (NVRs), digital video recorders (DVRs), and network storage (NAS/SAN/etc) devices. The popularity of household television program recording systems such as TiVO, or cable-company recording capabilities, is highlighting the NVR/DVR functionality. Mainstream I.T. departments are familiar with NAS/SAN, Blu-ray, RDX, and digital data tape (such as LTO IBM-TS, Oracle T10K) storage mediums and understand the utilization of these storage mediums in a video surveillance solution.

NVRs and DVRs, as well as NAS, SAN, and IP-SAN technologies, all have a finite storage capacity. Digital data tape technologies should also be considered when determining the storage resources available to a video surveillance system.

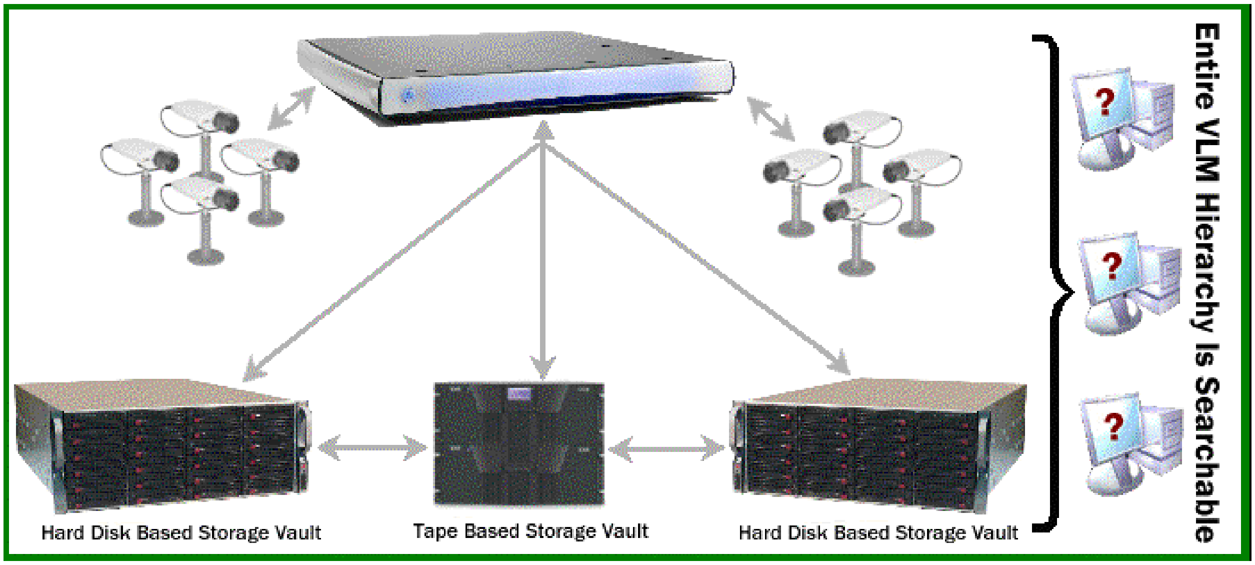
Best practices for data storage takes a more long-term retention view of video storage along with a modern, multi-tier, approach for the best storage management practices. Best practices avoid pre-determined DVR or NVR storage limitations in favor of more time-tested storage technologies such as optical media and digital data tape. It is the underlying video management software (VMS; see Section 6.4) that will ultimately utilize all available storage mediums available within an organization’s infrastructure.

It is in this combination of hard-disk, optical media and/or digital data tape that an affordable, viable video surveillance solution is created in a multi-tiered data storage infrastructure. This implementation also achieves the best economies of scale, longest retention polices, lowest cost of capital asset expenditures, and lowest total cost of ownership. This multi-tiered storage design provides for rules and policy-based video asset management that allows for best video retention and long-term retention capabilities.

7.7.1 Advantages of multi-tiered storage

Multi-tiered storage allows for greater scalability and can consequently support small surveillance systems as well as those with hundreds of cameras, which are also continually growing. Having a multi-tiered storage infrastructure on a single network reduces the overhead and maintenance costs of separate “islands” of storage. Where practical, being able to share networking infrastructure components significantly reduces the capital expenditure needed for a complete solution installation. Centralized management is another advantage of a multi-tiered storage infrastructure as the network can be accessed from a remote client to perform any maintenance or troubleshooting needs.

Redundancy and reliability can be easily implemented in a multi-tiered storage scenario removing any single point of failure. A few DVR/NVR solutions could become individual components of a greater multi-tiered storage infrastructure. Determine if a potential DVR/NVR system your organization may use could ultimately become a part of a multi-tiered storage solution.


Hard Disk Based Storage Vault
Tape Based Storage Vault
Hard Disk Based Storage Vault
Entire VLM Hierarchy Is Searchable

An example of a de-centralized multi-tiered video retention solution providing affordable TCO. An RDX jukebox could also be included in the storage resource mix.

8 Conclusion

Addressing best practice methods for implementing the overarching capabilities of the video storage management aspects of a video surveillance infrastructure provides an organization with an affordable, scalable, and easy to manage solution.

Some of the features and benefits of a best practice video surveillance solution include:

- Provide fully managed multi-tiered storage of all recorded video files
- Provide scalable long-term retention
- Easily connect and configure any IP-camera
- Automatically create low-res companion files of high-resolution video files
- Retain unaltered untouched hi-resolution originals fully intact (chain-of-custody)
- Utilize megapixel cameras without sacrificing storage capacity
- Enable extensive search and playback via expandable metadata
- Motion detection histograms for relevant searches
- Support powerful and intuitive Search / Playback / Export functionality
- Enable the end-user to quickly and easily find specific “events of interest”
- Enable offline media to be fully searchable and viewable
- Support extreme scalability
- Scan through the entire video file
- Search for specific “events of interest” with integrated analytical metadata
- Reverse, play, and fast forward with adjustable viewing speeds
- Create ‘start’ and ‘stop’ points in order to create segment “clips” for exporting
- Create as many segment clips from the same video as needed

9 Resources

- ABA Standards for Criminal Justice, electronic Surveillance, Section B, 3rd ed. 1999
- Guidelines for Public Video Surveillance, The Constitution Project, Washington, D.C.
- Bright versus United Corp., 2008 WL 2971769 V.I. July 22, 2008
- Jim Appleton, Trial Expert Witness in Video Imagery, Dallas, Texas
- Bill MacKenzie, Regional / Federal Account Manager at DITEK Corp