

## Why Storage is the Culprit in DVR Failures – and What Intransa Is Doing about It

June 2008



Digital video recorders are the backbone of video surveillance systems. However, DVRs, NVRs and the like are hugely dependent on one single point of failure: their individual hard drives. That these drives frequently fail is not even an industry secret, as it happens so often that it has become a cost of doing business. In spite of this severe failure rate, DVR vendors are not addressing the issue.

Why the strange silence? Because the DVR makers sell DVRs, not data storage; and they do not want to highlight DVRs' single biggest point of failure. This may be a good short-term business decision for them, but long-term it is causing enormous headaches for DVR users, and hurting businesses that depend upon video data. Now more than ever video surveillance is responsible for continuously recording *and retaining* vast amounts of images. Short retention periods mandated by limited capacity drives cannot serve this new business reality. Even worse is the plain fact that these hard drives fail. The hard drives that come attached to DVRs and NVRs were never meant to continuously receive large blocks of data images. When the hard drive crashes then the incoming video channel is down as well, not to mention the expense of replacing the drive or even the entire unit. The lack of reliability and adequate retention— plus lower resolution images because of the storage bottleneck – are seriously compromising the security practitioner's ability to get the job done.

Networked storage vendor Intransa has stepped in with a way to painlessly upgrade existing DVR/NVRs, eliminating their dependency on lightweight hard drives. Intransa preserves existing units by simply replacing failure-prone hard drives with economical and shareable security-grade external storage. This allows surveillance practitioners to avoid unit failures and field replacement headaches, while simultaneously greatly increasing resolution and retention.

### Why DVR Hard Drives Cause the Most DVR Failures

Video surveillance systems -- whether CCTV, DVR, DVR hybrids or NVR – need to be rock-solid reliable. But the hard truth is that in practice they are not. This is due to one overwhelming reason: *video systems save video to hard disk, and when the hard disk*

*fails it takes the system with it.*

This level of failure is so endemic in the video surveillance world that it is even considered a cost of doing business. Yet that cost is climbing higher and higher, and if it is not already unacceptable in your industry then it soon will be. Picture this:

**S O L U T I O N B R I E F**

- A casino DVR stops recording a game table because the recorder's hard drive fails. By law the casino must shut down the table until the hard drive is replaced and the DVR starts recording again. The casino's DVR repairman arrives within the hour with a spare disk, which is lucky. Thousands of dollars were already lost and any more time would have lost many more.
- A bank routinely videotapes ATM customers and transactions. One night a DVR hard drive fails so an ATM camera records no video. Unfortunately a customer withdrawing money from that ATM was robbed at gunpoint and there is no video of the crime. The detectives are unhappy, the bank's reputation suffers, and its attorneys prepare for a lawsuit.
- A major international airport adopts advanced video analytics. It is an exciting new development until they realize that the hard drives that are directly attached to the video recorders are regularly failing and losing the channel feeds. The loss of video cripples analytics and weakens the airport's investment.

Yet in spite of these serious threats, reliable data storage is the last thing many DVR owners and manufacturers think about. In fact, inadequate DVR hard drives result in even more problems than lost video. We can think about this in terms of three primary characteristics: reliability, resolution, and retention. The impact is the same whether

the hard drive is internal to the DVR or is attached directly to one of its ports. We refer to this type of storage as direct-attached storage, or DAS.

**Problem #1: DAS Destroys Reliability**

How reliable is a DVR? If it writes to a direct-attached hard drive as most of them do, the answer is "not very." DVRs are built from industry-standard PC components. This is not a bad thing as it keeps costs down and makes them simple to manufacture. But these standard components include hard drives made for everyday PCs. A PC's job is to intermittently read and write small files: word processing, spreadsheets, maybe digital editing. It is not running 24x7. But DVRs do run 24x7 under large data loads, and their hard drives were never meant to bear up under that kind of workload.

Making matters worse, if the DVR is recording video on an internal disk -- its one-and-only hard drive -- then it is recording on the same disk that also holds the PC operating system (OS). That drive comes pre-loaded with the OS and all of its files, as well as all of the software that turns the PC into a DVR. Not only do these pre-installed programs whittle down storage capacity from the start, but also when the overloaded and overused drive fails from continuously writing video it takes the whole DVR down with it. Is there anything else wrong with the DVR besides the hard drive? No -- but that does not matter, because the machine will simply stop working until its attached storage

**S O L U T I O N B R I E F**

is replaced. Whole channels cease to function because they cannot store their feeds, and some DVRs do not even alert security practitioners that there is a problem.

Even if the manufacturer attaches an external disk to the DVR just for video storage, those drive types are the same type as the internal hard drives. Even if the internal drive with the OS is running, if the external drive fails then the channel streams are a dead loss until the storage disk is replaced. That might take minutes if the security practitioner keeps extra hard drives in stock, hours if he does not, and days if he has no way of knowing that the drive has even failed.

And even if the drive does not fail outright, it will slow down under pressures like fragmentation. Because incoming channel data files are large and continuous, the drive has to keep placing incoming data to available sectors and moving older files around to accommodate the newcomers. In a short amount of time the drive becomes made up of widely scattered files and sectors, causing the drive heads to physically dart from sector to sector to write or restore data. This badly retards write and read times, causing the DVR to slow down considerably.

**Problem #2: DAS Limits Resolution and Retention**

Outright drive failure has the most significant impact on video surveillance, but there are other grave consequences as well.

The lack of storage capacity and performance affects operations like resolution, frame rates and retention periods. This makes video surveillance much less effective than it can and should be.

Where resolution is concerned, modern cameras are capable of high CIF ratings. High resolution leads to powerfully useful video for viewing and analytics, but unfortunately resolution is limited by storage capacity. If the DVR only has 500 gigabytes (GB) available for storage, and if most video must be kept for a minimum of 30 days, then there simply is no room to store high resolution video. It does not matter what the cameras are capable of or that video analytics need high resolution video. Storage attached to the DVR does not have room to store the files, so that is that.

In addition to limited capacity, direct-attached drives read incoming data much slower than the network can send it. This means that even when the cameras and networks are capable of handling high frame rates, they are bottlenecked at the disk storage level.

Retention periods are also badly impacted by limited storage capacity. In a world where video was stored for 30 days and then deleted, retention did not have a large impact. However, in these days of increasing regulations and extended retention periods, storage capacity becomes a major issue. Yet direct-attached DVR storage finds it difficult to impossible to yield longer retention. Video

S O L U T I O N B R I E F

continuously writes to the storage disk. Because there is finite capacity on the disk, older files must be displaced or the new stream cannot be written. This means that older video is only kept as long as there is room for it, which makes years-long retention impossible. And even when older video is backed up onto tape, retrieving it for viewing from large off-site vaults is a cumbersome, time-consuming task.

### **It All Adds Up to One Big Problem**

Reliability, retention, resolution – or the lack thereof – is directly related to poorly performing DVR-based storage. Due to the loss of the channel feeds, compliance audits fail. Crime is not recorded or prosecuted. Industrial processes go wanting. Personal injury claims cannot be proven otherwise. Depending on the nature of the industry using the DVRs, these consequences can range from minor to business-threatening.

But here is the good news -- DVR failures are NOT simply a cost of doing business. Unlike death and taxes, the most common type of DVR failure – a downed hard drive -- is *entirely avoidable*. How? By easily and economically replacing DVR-attached hard drives with a networked storage system. The system creates a powerful but easy-to-administer storage pool serving multiple DVRs. The problems of disk reliability, low resolution and frame rates due to limited capacity, and short retention periods are solved -- *without replacing existing DVRs*.

## **Networked Storage for Video Surveillance**

Before we describe the details of a particular storage system, we will take a moment to talk about networked storage in general. Video surveillance is a crucial element to corporate and consumer security, and is simply too important to trust to individual hard drives prone to frequent failures. Networked storage is the basis of a solution to the problem, but not all networked storage is created equal. The two primary types are Storage Area Networks (SAN) and Network Attached Storage (NAS). There is a good deal of confusion about the differences between the two types. It is important to understand those differences because the choice has profound implications for video surveillance storage.

- **Network Storage Type #1: Storage Area Network (SAN).** The important thing for security practitioners to be aware of is that SAN stores data in what are called blocks. Block-based storage is faster than file-based because the SAN does not need to inject its own file system layer in order to write and read video data. SAN-type storage is ideal for continuously writing large video datasets.

There are two types of SANs: expensive Fibre Channel SANs that are targeted to large data centers, and IP SANs that overwhelmingly suit video surveillance. IP SANs sit on the company's Ethernet network and easily store all networked

## S O L U T I O N B R I E F

data traffic, including traffic coming from the DVRs or NVRs. Many SANs can easily expand by simply adding more disks so the storage pool is never scattered around individual isolated drives.

The SAN disks are designed to automatically store copies of each other's data. This means that if a single disk fails another disk in the same pool automatically takes over. No data is lost at any time. This makes SANs ideal not only for reliably storing channel feeds from the DVRs, but also for quickly restoring video on demand. And IP SANs are far less expensive and easier to operate than Fibre Channel SANs.

One of the leading IP SAN vendors is Intransa, whose SAN serves the video surveillance industry.

- **Networked Storage Type #2: Network Attached Storage (NAS).** Security practitioners may already be familiar with NAS because of its advantages. A NAS is a collection of linked-together hard drives that serve as a common storage pool for multiple networked PCs. NAS is popular because lower end machines can be economical and fairly simple to deploy. However, when it comes to video surveillance NAS is a very poor choice. This is because NAS stores data in file formats, for example ".doc" files for Microsoft Word or ".xls" for Microsoft Excel. But video images do not come in tight little file segments that

can write directly onto the NAS hard drives. Instead NAS must add its own file system layer onto the video images in order to store them. This slows down the write/read functions of the NAS considerably and makes storing and restoring the surveillance images unbearably slow. It can also be very difficult to combine NAS boxes into larger storage pools, so large amounts of video end up being separated between individual NAS boxes. This makes it hard to know where video images are stored, which makes viewing much harder than it ought to be.

### **Intransa for Video Surveillance**

Intransa scalable, security-grade IP storage is the company's IP SAN offering. Intransa storage offers the following serious advantages to the security practitioner:

**Painless installation.** Intransa storage does not replace your existing video surveillance environment, it upgrades it. It deploys right alongside existing CCTV, DVR and NVR systems and leaves cameras, cabling, and video management in place. When the system needs more storage capacity, it is a simple matter to add additional disk or chassis to increase disk capacity. Intransa storage grows from 4 terabytes (TB) of storage up to 1,500TB without losing high performance and data protection abilities.

**S O L U T I O N B R I E F**

**Protect data from loss or corruption.**

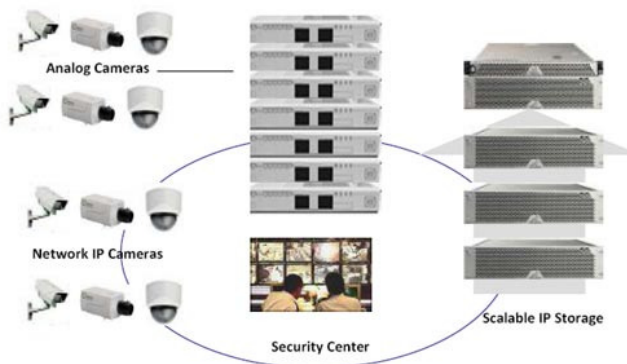
With traditional DVRs, the most frequent cause of failure is a failed disk. The DVR stops recording and the security practitioner may or may not be able to restore previously stored data from the failed drive.

**Automated management and protection.**

Once your security integrator has deployed the Intransa DVR upgrade, its automated SAN management feature kicks in. The feature is aware of drive or component failures as they happen and will immediately alert you with an email or network message containing the details. Automated management will also immediately shift storage away from the failed disk until it can be replaced.

**RAID protection.** Even if a drive fails the SAN will not lose data thanks to RAID5. RAID5 securely shares data around multiple disks. If a drive fails in the Intransa storage, RAID5 enables the system to automatically find and replace this drive with a spare without any data loss. While a few DVR models already come with internal RAID3 which is better than no RAID at all, it offers considerably less data protection than does RAID5. RAID on direct-attached storage is also quite expensive because it cannot be shared among DVRs.

**Superior system.** An external security storage system offers tremendous advantages, but may seem difficult to manage and deploy. Intransa simplifies the process for security professionals who are not storage professionals to easily add external storage to their existing security infrastructure.



Intransa IP SAN also comes with Video Storage Administrator (VSA). VSA graphically displays clear procedures that are customized for video surveillance users, meaning that security professionals never have to become storage experts. The SAN also

comes with built-in features like storage calculators and the ability to manage the SAN from a remote location, making VSA a key advantage of the Intransa IP SAN. But even though the system appears simple from the user interface, behind-the-scenes advanced features allow the SAN to manipulate storage to best serve video requirements. This allows security practitioners to affordably retain more video for longer periods of time, at higher resolutions, without fear of system failure.

In addition to powerful system software, Intransa storage uses server-grade hard drives to reduce disk failures by over 60%

**S O L U T I O N B R I E F**

compared with standard DVR hard drives. Because Intransa drives are hot swappable, they can be dropped in and will start running immediately without any downtime. Intransa tests and certifies SAN hardware and software to ensure full integration. Intransa storage was designed with bandwidth in mind right from the start, making it well suited for large video surveillance data streams.

By putting these features together, DVR reliability is no longer dependent on failing hard drives but is assured by an always available storage pool. Intransa offers full RAID protection and redundant systems so that no video is ever lost. And because pool capacity easily scales without impacting performance, security practitioners can take full advantage of new capabilities like facial

**Return on Investment: Benefits**

Benefit 1: Reduce costs and downtime by pooling video storage	Save 20% on video storage costs by pooling storage for DVRs and DVR groups. Easily customize storage to specific DVRs and their different needs.
Benefit 2: Storage upgrades do not shut down DVRs	Adding more drives to the SAN does not disrupt DVRs. Simply plug the new disk drives into the chassis or connect another chassis to make a storage cluster.
Benefit 3: Speed up storage performance	Direct-attached storage not only fails frequently but also slows down recording speeds, especially in otherwise high performance NVR. Storage pooling and RAID disk level striping speeds up video performance considerably.
Benefit 4: RAID makes storage extremely reliable	RAID5 is a standard feature on Intransa IP storage systems. RAID5 keeps disks always available and recording, so a failed disk never takes a DVR down with it.
Benefit 5: IP SANs make it simple to upgrade DVR to NVR	NVRs offer more features than DVR including scalability, megapixel camera support and video analytics integration. If you upgrade to NVR then the IP SAN moves up right along with you.

**S O L U T I O N B R I E F**

recognition that depend on higher resolution and frame rates. Higher capacity also allows practitioners to safely retain data according to its set retention schedule, not according to the inadequacy of the storage disk. Longer retention on the IP SAN also keeps data immediately available for playback.

### **Scenario: Baxter International**

Let us put this all together in a real environment. Baxter International needed to transition from analog to digital IP technology. The existing system consisted of 130 access control card readers, 100-plus fixed and PTZ analog cameras, seven DVRs recording 24/7, and an addressable fire monitoring system.

Baxter installed an Intransa SAN that eliminated video loss, more than doubled video storage capacity, and created a storage platform that can expand as requirements grow. By deploying Intransa IP storage, Baxter was able to easily migrate to digital technology by adding 20 new network cameras and replacing 25 analog cameras with new network IP versions.

In the meantime, the Intransa SAN supports equipment yet to be swapped out. Seven existing DVRs are still in operation. Originally they supported 500GB of storage each. Now that Baxter has added the Intransa SAN, the DVRs continue to search and serve the video just like they always did. However, the video that comes into the DVR from the analog and IP network cameras is

written directly to the IP SAN. This has greatly improved DVR performance and reliability.

The upgrade process is simple: each DVR is equipped with a network interface card to connect via IP as part of the easy upgrade process. Baxter is free to use the DVR's original video management software or a new video management system (VMS). The Intransa SAN supports both, meaning that existing cabling, cameras, DVRs, and procedures remain intact. Baxter can also increase SAN capacity by adding disks as needed without taking any equipment offline.

### **Taneja Group Opinion**

A lot is riding on video surveillance these days. In this era of increasing regulation and longer retention periods, poor recorder performance or outright failure has increasingly bad consequences for the businesses and governments that depend on reliable security video. There are two keys to remedying this threatening situation: 1) replace outdated direct-attached hard drives with economical IP SANs and 2) install an IP SAN that preserves existing investment by working with installed video recorder equipment.

These two points together have a huge impact on return on investment (ROI). A good ROI is an important goal for any workgroup or business, but is particularly important for security practitioners. As important as video surveillance is (and it is),

**S O L U T I O N B R I E F**

security budgets have been historically flat and equipment is expected to last. By installing an IP SAN, practitioners immediately gain rock-solid reliability along with support for high resolution and required retention; all of which greatly increase the return on investment. In addition, Intransa upgrades to existing recorders are simple and non-disruptive. This allows businesses both

to leverage existing equipment, and also to support higher resolution and frame rates.

There is a good reason why IP SANs are becoming a major force in video surveillance. Intransa encapsulates these reasons in their ROI-focused approach to storing invaluable data for video surveillance systems.

---

*NOTICE: The information and product recommendations made by the TANEJA GROUP are based upon public information and sources and may also include personal opinions both of the TANEJA GROUP and others, all of which we believe to be accurate and reliable. However, as market conditions change and not within our control, the information and recommendations are made without warranty of any kind. All product names used and mentioned herein are the trademarks of their respective owners. The TANEJA GROUP, Inc. assumes no responsibility or liability for any damages whatsoever (including incidental, consequential or otherwise), caused by your use of, or reliance upon, the information and recommendations presented herein, nor for any inadvertent errors which may appear in this document.*