intransa®

The Security Convergence Market

How a New Era of Global Risk Elevates Security Policy and Creates Opportunities for IP Network and IP Storage Architectures

April, 2007

An industry brief

by Dan Dunkel
New Era Associates, LLC President

White Paper

Abstract

Corporate security has become a high-profile issue since the events of September 11, 2001 forced a redefinition of the traditional concept of risk. No area has seen more growth and increased demand than video surveillance as part of that redefinition.

As a direct result, the security function in corporations is in the process of evolving and creating a new value proposition, which enables a "trusted enterprise" model. This trusted enterprise involves both internal corporate operations and extends outward to multiple partners, comprising global supply chains.

"The risks we will face in the future will be new, complicated, serious, widespread, and extreme. In fact, there is an entirely new definition of risk emerging made up of the totality of threat factors, requiring new thinking about what risk is."

- Dr. James Canton, "The Extreme Future", 2007

For the most part, this fundamental industry change is lost on the majority of traditional physical security practitioners, manufacturers, and their integration channel partners who have limited exposure to senior management in major corporations. However, this business reality is the driving force behind the increasing presence of major IT (information technology) vendors, such as Cisco and IBM, and their strategies to embrace the security convergence opportunity. They are using this window to position the decision cycle for physical security applications involving the convergence of voice, data, and perhaps most importantly video, away from traditional security operations and into the IT departments and the CIO (Chief Information Officer) suite, where they have strong, historic business relationships long established.

It makes economic sense that the security department would eventually join the ranks of every other business unit in the company as a customer of IT, rather then being standalone, and often times employing proprietary installations. In many ways, the physical security department, while operationally critical, is effectively the last domino to fall in regards to utilizing open systems, interoperability, and web access, all of which are commonly offered by IT. The larger opportunity is at the middle and higher end of the market.

As an example, smaller installations for video surveillance deployments such as elementary schools and parking garages today require expensive coaxial cable deployments. These will increasingly be replaced by IP-based (Internet Protocol-based) wireless systems. For traditional vendors, price points as well as margins will erode quickly.

As a result, the physical security integration channel is in a state of increasing flux. Many have valuable video surveillance and access control experience, but lack in the fundamentals of IP networking and storage strategies, leading to this challenging situation.

Aside from understanding that the security function is being re-positioned at the highest levels, it is also important to recognize how these changes are impacting traditional physical security product development cycles, sales channels, and partnering strategies moving forward. The fact is that over 80 percent of America's critical infrastructure is managed by the private sector. Protecting the homeland is becoming politically correct, and corporate security managers have an essential role to play in the protection of key industries and the physical, electronic, and human assets that comprise them.

The core of security convergence is the ability to accelerate the deployment of security policy (solutions and management) across the IT infrastructure. Major components of this infrastructure are IP networking and IP storage, for the most part foreign to the physical security industry.

With the Intransa StorStac System providing scalable IP networked storage that security systems integrators, solutions providers and vendors can leverage as the storage platform for their solutions, companies are able to ensure their survival and continued well being in this new, rapidly evolving marketplace.

1.0 Executive Summary

"The global security industry, combining both products and services reached approximately $150 billion in sales in 2006."

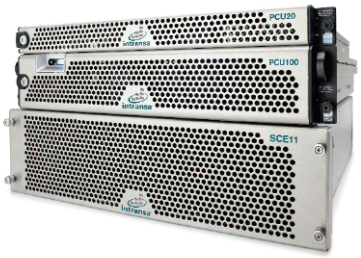
– Lehman Brothers

One interesting sidebar to the above market data is that almost half of total revenue is represented by physical security guarding services. Perhaps no other segment of the physical security industry is therefore as ripe for a convergence strategy as what we sometimes think of as the second oldest profession in the world, physical security. In fact, we are seeing increasing levels of software automation in the disciplines of command and control and next-generation intelligent video surveillance solution delivery.

While industry statistics support IP networking and IP storage technology's ability to deliver a platform to the video surveillance market aggressively, the ultimate upside may in fact be the integration of additional open security applications, utilizing video data mining techniques often called video analytics), onto a scalable storage platform.

The future of the security application market appears to have video as a base requirement for identity management and verification systems. Clearly, integration is both the keyword and the key skill for the security integration channel moving forward.

Intransa offers a scalable IP network storage platform that is ideally suited to supporting streaming video applications, specifically video surveillance.



The scalable IP network storage offered in the Intransa StorStac System is modular, with full RAID 0, 1, 5 and 10 support for even the most demanding video surveillance application requirements. Intransa platforms offer centralized administration and management, whether supporting a few dozen cameras in one or a few locations, or several thousand across a country or continent.

Capable of supporting "edge" devices in individual clusters of digital video cameras, through to tens of thousands of cameras with centralized management and a repository for video analytics and other purposes, Intransa IP network storage is likely to be the platform of choice for security integrators, resellers, developers and vendors to base their traditional and newer, evolving solutions.

Market Research: A quick review

- The U.S. Department of Homeland Security's FY06 budget earmarked $51.1 million for the America's Shield Initiative, which enhances electronic-surveillance capabilities along our borders. This represents an increase of $19.8 million over FY05. As we head toward 2008, securing the homeland remains a political focus and necessary reality.
- IMS Research forecasts that the Video Analytics market will explode over the next five years, growing from $67.7 million in 2004 to $839.2 million in 2009, and at a Compound Annual Growth Rate (CAGR) of 65.5%. Only by using scalable IP storage solutions will security vendors and solution providers be able to address this market opportunity.
- The worldwide Internet protocol surveillance market will grow to $6.48 billion in 2012 from last year's $435.8 million, according to a report by Frost and Sullivan.
- Global Video Equipment & Installations reached $6 billion in 2005 according to Lehman Brothers. This does not including consulting services which generate three times the revenue of product sales. For example, IBM is on record as saying they will generate $3 in integration services for every $1 of video surveillance equipment sold.

"Since 2002, 2 million surveillance cameras have been deployed in U.S. annually, and each unit adds hundreds of hours of footage to be organized, analyzed, and archived."

Recognizing this is core to traditional IT storage vendor EMC's apparent strategy for the security convergence market.

- "Companies are increasingly migrating their security and surveillance systems to IT-based storage platforms."
- Joe Tucci, CEO, EMC

- "The Worldwide market for identity management software will increase by 47% annually, reaching 4 billion dollars by 2007."
- IDC

One major advantage for IT vendors and integrators entering the security convergence market is that the current security industry in many ways is a mirror of the IT market of ten or even fifteen years ago, especially when considering storage architectures.

Today's DVR and NVR systems are akin to the departmental PC server, which populated corporate America prior to the advent of basic NAS (network attached storage) and more powerful SAN (storage area network) architectures.

IT changed dramatically with the advent of these technologies. It was not that the PC platform did not function properly; it did. But the true issues were more along the lines of initial architectural intent and administration cost of these individual PC systems.

As we know, the original IT servers also evolved from an architecture that was designed to be a desktop workstation. As a result, limitations in scalability and performance followed, and required multiple installations, maintenance, and led to major administration costs. We will explore similar issues when reviewing DVR and NVR technology in a following section.

The point is that this tracking of IT history does not end with storage server technology. The same deployment strategies that allowed engineering departments to break the bonds of proprietary and standalone installations are at work in the physical security market today. It is like stepping into a time warp and replacing 2D drafting tables with 3D workstations. The same selling concepts of employee productivity, ROI (return on investment), and collaborative workflows, apply.

The interesting or frightening thing, depending upon your organization's perspective, is that these selling techniques are new to many physical security vendors and their channels. This explains in part why this industry practically throws its arms up and exclaims, "There is no ROI for physical security". Certainly this remains the case in terms of standalone proprietary hardware and software installations.

While touching on the subject of sales channels it is important to note the hands off, rather than arms length, strategy deployed by many well-known physical security manufacturers. Some of these major security vendors are blocked by regional or local resellers and distributors from any contact with the end user customer.

The author personally witnessed an exchange between a product VP at a multi-billion dollar access control and video surveillance provider and an IT Director of a well known, major convenience store chain.

The customer essentially told the product VP that they needed another layer of management between their own reseller and headquarters to escalate customer product requirements (which the reseller refused to do). The VP told the author afterward, "There is nothing I can do, the reseller owns the account". We told him to hire a sales executive with IT experience to show the company and their industry how to run a sales channel. The lesson learned is not to assume business as usual in the physical security channel. Instead, set the ground rules and maintain customer relationship and contact from the outset as a support requirement.

The fact is that digital video surveillance is the future direction for many reasons, not the least of all is that the transformation from analog to digital adds value through integration with other applications.

We are increasingly seeing video being used in tandem with access control applications. One future direction in this area is incorporating facial recognition software into the process. The ability to match a mug shot photograph against a video stream in real time and access video storage through data mining is on the horizon. That technology will need to massive amounts of storage, much of it maintained over the long term, and with centralized control.

"As the security industry transforms to one that is based on open standards and IT infrastructure, video data moves to file based formats. By keeping video longer and using sophisticated video analysis tools, new and different trends can be uncovered. Video data mining is on the brink of being real."

– Len Johnson"Video Evangelist", IBM

The ability to store large volumes of video data is a critical component of how surveillance software will integrate into future security application functionality. Identity management and access control systems are at the heart of the concept of "Trust but Verify", and these applications are getting more visual. Storing everything from fingerprints to voice prints, to photos, to the actual gait (walking style) of individuals will be incorporated into personal identification and verification policy in the future. A wide variety of biometrics will replace access control cards for physical entry and log in and passwords for electronic privileges. The number of security solutions accessing video data files is increasing and lengthens storage needs and requirements.

Collaborative voice, data, and video traffic will require a scalable and flexible IP networking and IP storage architecture. Think of the automation that is taking place in the commercial, or "intelligent" building industry as a starting point. Intelligent buildings are a combination of physical barriers, networked video surveillance and access controls, which include total integration into HVAC control systems operating with smart sensors to turn off lights and adjust thermostats based on room occupancy and other pre-set factors.

2.0 Introduction

Security as a profession is taking a quantum leap forward in tandem with the technical advancements of the twenty-first century. We will look back a decade hence and realize these initial stages of physical and logical security convergence truly changed and repositioned an age-old industry. A new era that redefines global risk will rely on a new generation of security professionals to establish the trusted environment required to succeed and thrive in a global community.

Collaboration will become the foundation for the next generation of security practitioners to create new innovations concerning the protection of physical, electronic, and human assets.

The security landscape is in flux, and convergence is driving the change. Not just technology convergence, but also functional, organizational, and skill convergence are taking place. This subject demands attention by the entire management team, from the CEO (Chief Executive Officer) and business unit managers to the CIOs (Chief Information Officers) and emerging, new-style CSOs (Chief Security Officers).

"Convergence is requiring our security leaders to learn much more about the business and change their perspective of their position, from a functional subject matter expert to a business person with functional knowledge."

-Christopher Kelly, Vice President, Booz Allen Hamilton

The management practice of traditional security is evolving from one of deploying tactical solutions to respond to issues, to one of strategic solutions to proactively protect business operations. Again, if we look to IT history as a guide we can track a similar progression to that of the Vice President of Data Processing in the early 1980's being primarily a technician and not a business person.

Today, the CIO who replaced that VP of Data Processing understands how each business unit functions and how technology can assist in the overall operational goals of the corporation or enterprise. Outside of the CEO, perhaps no other executive interfaces as closely with the business units as the Chief Information Officer.

The CSO is undergoing a similar transformation today. An astute security solution sales professional will bridge the gap between physical security and IT executives and management to leverage their unique contributions toward the overall protection of the corporate assets and business operations.

In many ways the CSO's responsibilities will continue to evolve based on the fact that providing a trusted enterprise model will require an extension of security policy outside of the organization and into the partner and supplier channel. The skill set of the next generation CSO places a priority on understanding how a holistic security policy effects business issues. It also requires being influential in dealing with boards of directors and senior management.

While experience in physical security or military operations can be a plus, the 25-year veteran FBI agent who leaves the bureau to ride out 5 years until permanent retirement as a corporate Director of Security is more than likely not the model moving forward. The new threat levels and risk to business operations, as well as a focus on ROI for security operations, are clearly driving the security convergence momentum forward, and changing who fulfills specific roles, and even to whom they report.

In fact, in some organizations a CRO (Chief Risk Officer) position is becoming prominent, based upon senior management impatience with the physical security and IT department's inability to find common ground. These risk managers serve at a considerably higher level than do security directors. In fact, most security directors do not report directly to the top management of their companies, while CROs do.

In some ways an analogy can be made between corporate security and national security. The security function is larger than just one isolated department. A CISO (Chief Information Security Officer) position is also evolving in large corporations, including at General Motors and E-Bay. It is almost a hybrid between the two positions of CIO and CSO, although usually reporting to the CIO, or in some cases both functions report to the CISO, company dependant.

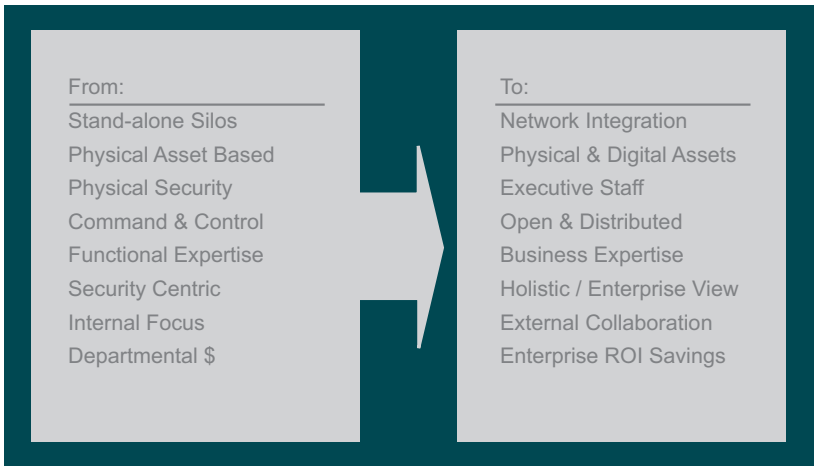
As the convergence of traditional security solutions and information technologies continues to gain momentum, numerous changes are occurring in the management ranks, which impact executive roles and responsibilities.

"75% of organizations have some form of integration between physical security and computer security, up from 29% in 2003 and 53% in 2004."

"40% have the same executive overseeing computer and physical security, up from 11% in 2003 and 31% in 2004."

- Pricewaterhouse, Coopers Survey

The New Security Model:



The bottom line is that a significant shift in emphasis from security as a purely functional activity within an enterprise, to security as a "value add" to the overall mission of business is occurring around security convergence. It is impacting everything from management structures, to vendor relationships, to product development cycles, and even extending to stakeholders and shareholders.

New technologies, such as IP storage, cannot be ignored but must be understood and embraced for vendors to survive. For many solution providers and security systems integrators, Intransa's IP networked storage will be the foundation for that survival.

3.0 Video Surveillance Background

There seems to be considerable confusion among end-users regarding digital video cameras. These devices, for the most part, are still in fact analog — they take the image, digitally process it, and then convert it back to an analog output for display.

These current digital cameras are cost-effective and installed in many security programs. They can offer improvements in low-light capabilities and better imaging over standard analog cameras. They are also a good fit for most traditional surveillance applications, but while all of that is true, they will eventually become obsolete as mega-pixel imaging becomes common, requiring significantly more storage.

DVRs (Digital Video Recorders) are hybrid technologies, part analog and part digital. Images are analog and delivered by coaxial cable to the DVR, where they are digitized, viewed, and stored.

DVRs were the first industry attempt to scale video storage. Unfortunately, they also inherently created the problem of too much data from too many cameras. Like IT disaster recovery scenarios, the issue is not the backup operation so much as the problem of restore time. Specifically in this example, the issue is one of available search time. Thousands of hours of tape every day or week must be searched to find a particular item.

This is old school technology and simply requires too much human intervention to be effective. These devices also expand in camera increments of 4, 8, 12, etc., so if one more camera is needed you must obtain and install additional equipment in those increments. This is the "brick" approach to surveillance cameras and storage, paralleling some basic IT solutions known as brick storage that are also similarly dated.

Some DVRs create software matrixes and many are using network storage by incorporating network video into the solution. The problem is that these solutions are not positioned for the explosion of storage and network bandwidth. While the DVR market still has an 80% market share (Security Info Watch, 2006), the author's belief is that within the next two years we will see the elimination of the need for digital video recorders (DVRs) altogether. New installations are moving away from this technology at the mid/high end of the market.

NVRs are essentially DVR technology positioned for the web. The NVR allows for expansion by adding an encoder device, while the DVR must be configured in groups. Over the past few years, NVR vendors have tried to gain a competitive edge over their traditional DVR counterparts.

Most NVR's are software based systems and can be installed on almost any standard server depending on capability. Many NVRs enable users to access, view and control surveillance cameras from anywhere on the LAN, WAN, corporate intranet or the Internet. The software can support video from analog, digital, and network cameras from a variety of manufacturers, including advanced imaging mega-pixel cameras.

The NVR system eliminates the need for a hardware matrix, multiplexer, switches and control panels. It can also be used very effectively for multi-site surveillance, as it enables centralized control of unlimited remote installations and offers offline storage of recordings, with full redundancy to secure locations.

This NVR technology offers improvements over DVRs for scalability and flexibility issues, but currently experiences the problem of searching large volumes of raw data, and can also encounter network bandwidth issues. Thus, this remains of limited value for video data mining or multiple application solutions.

Network video offers the most flexible video solution, but brings concerns about bandwidth use and network security. This technology is excellent but not as widely deployed due to the lack of security industry understanding of IP in general.

Solution vendors are able to leverage the IP expertise of Intransa, shipping IP storage solutions since 2003, in order to train themselves and their integration partners on appropriate IP networking and storage fundamentals, thus effectively building a captive audience of dedicated partners to sell their own solutions.

What is a Video Server?

A video server digitizes analog video signals and sends digital images directly over an IP network such as a LAN, WAN, corporate intranet or the Internet. It essentially turns an analog video system into a network equivalent, and enables users to view live images using a standard web browser or video management software on any local or remote computer in a network. It also allows authorized viewers from different locations to simultaneously access images from the same analog camera, as well as network cameras as they are added to the system.

In this market, Axis Communications is the adoption leader. Their network video products are designed with built-in computers, so they do not require a direct connection to a PC or any additional software to stream live video and audio over networks. Instead, Axis users simply connect the network video cameras to an IP network and view live images.

Important Note: *IP cameras use motion JPEG or MJPEG to encode video. The problem with this format is large storage requirements compared to MPEG 4. Some newer systems use MJPEG for video analysis and MPEG4 for storage (3VR).*

Advanced Video Imaging

New mega-pixel camera technology is an important advancement and enables higher resolution and more functionality to actually process the video and to view independently from one another.

This technology gives the user control over the image, and also enhances the abilities of some advanced software solutions. Video analytics is an example of an intelligent surveillance software offering that analyzes or examines video for specific things. The industry overall is moving toward more system intelligence and software platforms.

Important Note: *Not all video surveillance software is "intelligent".*

Many installations / solutions do one function well, such as facial recognition or motion detection, and provide a single added feature to an NVR.

Surveillance software is growing more intelligent in order to reduce the amount of false alarms, often a problem with motion detection. For example, some new software knows the difference between a man crawling on the ground and a dog looking for a bone.

Intelligent systems can also analyze archived video to identify patterns and trends such as unusual human behavior, suspicious vehicles, lights turning off and on, and other observable activity. This ability to learn and respond makes intelligent software indispensable for security operations.

"In the digital migration, the first move was from the analog VCR to the DVR,"
Jeff Stringer, ADT's director of retail technology sales, told the author.

"We used to think if we could create a DVR with the capabilities of a VCR, we were doing good. Now the power of video analytics has moved this frontier in a totally new direction. We are amidst a constant redefining of video analytics to create a business management tool. We moved a few years ago to motion, movement of items and the ability to search for moved items and light change. We have recently added object size, speed and direction."

The next generation of systems will involve integrated analytics into existing and new data and video databases. An example would be matching a photograph such as a mug shot against a streaming video of a subject who may prove to be a criminal or terrorist, while entering a convenience store or an airport terminal. Software upgrades will grow to be a simple network download. And interoperability between remote locations will automatically track movements and an open architecture to integrate with other applications.

A quick example of the new security surveillance ROI is that smart video is transforming digital video recording from a pure loss prevention device into an operations management tool. A major, leading home improvement chain had three objectives in mind:

First, to ensure a safe and secure environment for its 300,000 employees and millions of customers;

Second, to stem losses from theft, fraud and error;

And third, to use knowledge gained through video recording to increase productivity and improve customer service.

Their installed system is designed to address all of these.

Surveillance video typically has dual use capabilities. For example, employee (cashier / security officer) training, and customer buying habits (marketing).

Overall, corporate America spends more than $34 billion annually on employee training, and these next generation systems will clearly become a part of that expenditure. Reliance upon a scalable IP network storage solution will increase for the same reasons.

4.0 Security Convergence Positioning

"The possibilities in an IP-linked surveillance world are almost limitless, which is why that market is set to explode."

– Frost & Sullivan

The term "convergence" has a long and varied history. In today's interconnected and global operating environment, it seems nearly impossible to follow developments in technology or business without encountering the word. When used in the context of commerce, convergence means that non-traditional elements of a business are starting to be more alike, with units coming together to create competitive advantage.

The increasing focus on security from an enterprise perspective has led to a new way of examining risks that institutions face as a whole. This, in turn, is leading to innovative approaches that emphasize integration—specifically, the integration of the risk side of business into the strategic planning side, in a consistent and holistic manner.

"In the past, management of the risk inherent in a business was a function embedded within the individual roles of C-level executives such as the CEO and CFO (Chief Financial Officer). The traditional approach was to treat individual risks separately. The problem with this stove-pipe approach is that it not only ignores the interdependence of many business risks, but also sub-optimizes the financing of total risk for an enterprise."

– William Crowell, former Deputy Director, NSA

Many of the trends are positive for the selling psychology innate to the IT industry, but not so well understood by traditional physical security practitioners. It is key to remember some core differences in attitudes regarding security and IT mindsets, many of which are diametrically opposed.

For instance, IT security has technical expertise but not large numbers of staff. Physical security generally has the opposite. Thus, both groups can benefit from each other, with the common ground of protecting the assets (physical, electronic, human) of the corporation or enterprise.

At the core of the issue is that security as a discipline is conservative and measured, even skeptical of human nature in some cases. Compare this to the aggressive innovation cycles in IT and the "insanely great" attitude of the industry. The geeks and guards (student demonstrators and campus police) analogies often discussed are not far off the mark. Add to the mix the fact that some security people feel threatened by the aggressive push into their industry by the IT vendor community, a lack of IP networking and IP storage understanding, and combined with shifting buying decision responsibilities, the result is a potential bottleneck to collaboration.

Some in the security industry feel that the IT industry is crashing the party and dictating the rules. However, security convergence can be explained to physical security personnel by pointing out an early example of physical security leadership.

Take for example an example from New York City. The NYPD in the 1980s, under Chief William Bratton and Mayor Rudolph Giuliani, established the Comstat system. They pioneered the use of computers and software to automate the process of updating criminal statistics in real time. The senior and middle management of the police department would meet in large sessions every week to discuss crime patterns and countermeasures to reduce incidents.

This collaboration streamlined communication between various internal departments across the police department (including narcotics, homicide, traffic, and vice), which up to that time had operated independently from each other. This is a clear example of a traditional physical security function (crime reporting) embracing convergence with IT to integrate within a traditional (silo) command and control decision-making model and improve it through real-time intelligence and management (collaboration).

As the security profession moves quickly toward integration with information technologies, the ability to leave aside traditional stand-alone deployments and leveraging centralized decision making will be a critical requirement for success. The physical security industry already embraced convergence over 20 years ago, and the rest of the market is beginning to catch up.

The continuing convergence of new technologies with existing business practices does create complexity and change. This underscores the importance of industry education and creates opportunities for entirely new products, marketing strategies, and but also competitive threats to traditional vendors and their sales and support channels. Leveraging the IP networking and IP storage knowledge and solutions from Intransa may be the difference between survival and profitability for many in the industry.

Industry Examples

Security convergence is driving industry change. For an example, consider the following:

- 20 Billion dollar Tech Data U.S. Helps IT Resellers Break into Physical Security; Physical Security SBU Established and Leading Manufacturers Signed (April 18, 2006)
- IT resellers and security system integrators can now leverage Tech Data Corporation to develop an array of the latest IP-enabled physical security and access-control solutions.

Cisco CEO John Chambers tells the Worldwide Reseller Channel, "We will be a video surveillance company within one year" – San Diego, CA - 2006

"The Network as the Platform for Safety & Security"

"Physical and Virtual Security will be impossible to separate in the future"

"The days of Silo Security Implementations are over."

"Stand alone System Security is a bottleneck."

"Security Solutions must take a Holistic approach".

"Basically, the IT industry has flattened out after many years of constant growth. So IT found a new growth area in the security industry which is becoming more and more like IT everyday as electronic technology applications advance."

– Joe Freeman, Freeman & Associates, March, 2002

4.0 State of Convergence - A Higher level View

The move toward IT governance is occurring simultaneously with the convergence of physical security solutions and IT within the context of an enterprise security policy. This intersection offers an opportunity for leading edge companies to compete in the new global economy with highly optimized IT infrastructures providing flexible business services, while at the same time offering a secure environment for protecting digital, physical, and personnel assets.

The convergence of security operations, both physical and logical, is embedded into the IT governance process as a critical business element. Leading edge organizations will merge IT governance initiatives, a flexible computing infrastructure, and global security policy into a "trusted enterprise" model. This approach provides the ability to proactively respond to business opportunities and protect against new security threats equally well.

This strategy will ultimately provide unique competitive advantage in the global marketplace where value is calculated on continuous innovation, time to market, and secure global operations. The trusted enterprise model can be expected to create a higher stock valuation for those enterprises which successfully deploy it. A well managed IT governance policy, which includes security as part of its vision for the future of business operations creates that foundation.

Security Convergence: Rules of the Road

Security and convergence are concepts that must be examined separately to gain an understanding of their combined business value.

Enterprise security policy integrated within an IT governance framework offers the best protection of global assets and human resources.

The security professional of the future will understand the impact of technical innovation and global business operations from both an internal and an external perspective.

Security convergence in a word is collaboration; it involves a shared responsibility for a sound defense of global assets and business operations.

The military soldier, first responder, and corporate employee of the future are children of technical interoperability and collaboration; this will change the global definitions of work, management, and risk.

The convergence of voice, data, and video over the global Internet Protocol (IP) network is accelerating a redefinition of the traditional electronic and physical security business models.

Convergence is the most significant trend in identity management practices and provides the foundation of the Trusted Enterprise Model.

The convergence of new technologies with existing business practices creates complexity and change. This underscores the importance of industry education and creates opportunities for entirely new products, marketing strategies, and competitive threats to traditional vendors and their sales and support channels.

At the core of the trusted enterprise is the basic understanding that security policy begins at the top, with the board of directors and the CEO.

In the future, the valuation of a company's stock and shareholder investment will be tightly aligned with its global security policy.

– Excerpt from "Physical & Logical Security Convergence, Dan Dunkel, Chapter 18

Aside from corporate mandates, the public issues involved with security solutions, specifically video surveillance and access controls, cannot be overlooked. Although the topic is extensive, it is interesting to follow the video surveillance history and trends of the United Kingdom for a view into the potential market adoption here in the domestic United States.

While it is true the battle with the IRA and their terrorist bombing campaigns in London underscored video surveillance deployments, the UK has a rich history in security leadership from the days of establishing the world's first formal police force to the initial use of mug shots and video cameras.

Dr. Stephen Graham, of the University of Newcastle upon Tyne, has suggested that video surveillance networks are effectively the "fifth utility", after telephone, water, gas, and electricity. "These networks," he writes, "have long since merged and extended to become technologically standardized, multipurpose, nationally regulated utilities, with virtually universal coverage".

The author would argue that CCTV (closed circuit television) looks set to follow a similar pattern of development over the next 20 years, to become a kind of fifth utility. In their book The Maximum Surveillance Society: The Rise of CCTV, academics Clive Norris and Gary Armstrong write "The architecture of the maximum surveillance society is now in place". Their point is that the hardware of CCTV is so firmly in position that enabling it to watch everybody all the time is now merely a software problem.

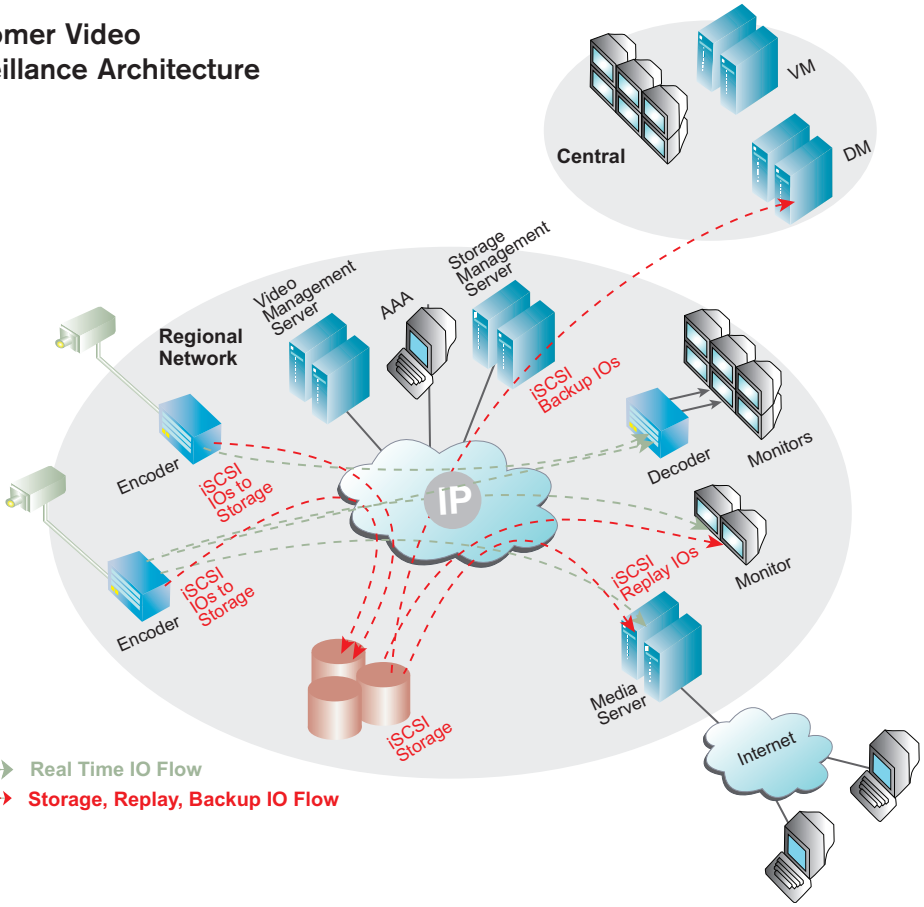
Today various estimates place the number of video surveillance cameras in the range of 4.5 million within the United Kingdom. Moreover, in the city of London, there are more than 500,000 security cameras, and video cameras have been in use there since the 1960s. The Wall Street Journal estimated that a person could expect to be recorded 300 times a day in the city, according to one study.

A fast-emerging direction for surveillance technology, and aligned with the above information, is using video as an intelligent sensor. New software has enabled users to not only view and manage video, but also to make corresponding informed decisions and responses through integration with technologies such as WMD (weapon of mass destruction) sensory devices.

Additionally, voice or sound sensor technology is being integrated into next generation software at the end point (typically a camera), providing the ability to hear shouting, car crashes, or gun shots, and then pan, tilt, and/or zoom the camera, producing alarms and security responses (emergency dispatch with video footage) accordingly.

To consider how the most advanced video surveillance systems of the future are already being requested by customers today, security system integrators, developers and vendors should consider their choice of platforms to move with the market. A scalable IP network storage solution, such as the Intransa StorStac System, is mandatory.

Customer Video Surveillance Architecture



Intransa StorStac Systems are the ideal IP storage platform for security systems integrators and developers to apply their software applications to. Beginning with 1Gigabit/second edge devices, supporting a handful of cameras each, through to 2 Gigabit/second for double the performance for real-time application needs, StorStac Systems also offer 10 Gigabit/second interfaces for the ultimate, high performance requirements of centralized management and video analytic support for 10,000 or more cameras.

The StorStac System scales from 8 through 800 terabytes of storage in a single system, and is architected to grow to 1 petabyte and beyond. What that means to security system integrators and developers is that while an initial StorStac System on the “edge” could be deployed to support 30 or 40 cameras, a completely integrated Intransa StorStac System could quite easily be the storage platform for 10,000 or more cameras, and all be centrally managed, regardless of physical location. Intransa provides the platform to make that capability a reality, based upon their proven IP network storage expertise, shipping products around the world since 2003.

5.0 Conclusion

The security industry is currently transitioning from an analog infrastructure to a fully deployed and global digital base. The current stage involves hybrid solutions to leverage existing investment in the infrastructure.

Over the next few years, the transition to digital systems will be almost complete. This will prove to be much to the surprise of many traditional physical security manufacturers and vendors, who falsely believe that security convergence will occur within traditional security industry product cycles of five to seven years.

Many multi-billion dollar physical security companies and their channel partners risk repeating the unfortunate history of the at one time very successful minicomputer industry, which went completely out of business and disappeared from the corporate landscape. Their loss will be the IT vendors' gain, as the current $150 billion security market continues on to explosive growth. And security policy will soon be as important to the value of a corporation as its IT infrastructure and e-commerce initiatives were during the late 1990's.

Simply put, security will become job one, and video surveillance will be a core utility in the process.

Leveraging a scalable, cost effective and centrally managed IP network storage system as the base platform for that video surveillance storage capability will become critical to the survival for security integrators, solution providers and vendors. Intransa offers just that technology today to developers, integrators and solution providers.

6.0 To Learn More

Since 2001, San Jose, California-based Intransa has been the leading innovator of IP-centric networked storage solutions, delivering independently scalable performance and capacity with high availability, outstanding price/performance, and proven ease of use. Intransa customers can be found around the world.

To learn how the Intransa scalable industry-leading IP networked storage StorStac System is the ideal platform for your video surveillance solution, plus how to leverage us through our StorPartner Channel and StorAlliance Business Partner Programs, please visit us at **www.intransa.com**, or call 408.678.8600 or 1.866.446.8726. We'll be watching

2870 Zanker Road, Suite 200, San Jose, CA 95134 ▪ t: 408.678.8600 ▪ 1.866.466.8726 ▪ f: 408.678.8800 ▪ www.intransa.com