Bp.IP™ Best Practices for IP-Based Systems

Ten Rules for Putting Your Physical Security Systems onto the Corporate Network

How Physical Security Departments Can Successfully Make the Transition to IT-Centric Systems

by Ray Bernard

v 1.6

Table of Contents

Introduction

For physical security technology, the initial convergence trend was to improve security systems by incorporating information technology (IT) enhancements. Now many security systems do more than incorporate IT elements, they are completely based upon them.

Security video technology is a good example. Before the 1990's tape video cassette recorders (VCRs) were used to record video images from vacuum-tube video cameras (whose glass video tubes work in reverse of a television video display tube). Today's video cameras are solid state (i.e. electronic circuit chip) devices, and can be characterized as a "computers with a lens".

Sony and others manufacture security video cameras that contain a hard drive for storing video, and a web server for providing web browser pages for displaying the recorded video. The cameras connect to a computer network via a standard network cable, and thus are classified as "network cameras". Many such cameras can be powered using *Power over Ethernet* (PoE) technology, so only the network cable connection is required to activate the camera.

Today's computer-like cameras send back video image data as network information packets using Internet Protocol (IP), and the information is stored the same way any other corporate electronic data is stored, often in a corporate data center.

Thus physical security systems infrastructure (computers, databases, data storage and networks) is actually IT infrastructure. Thus is should be no surprise that the physical security industry's largest customer, the U.S. Federal government, has in essence declared that physical security systems are IT systems.

The Security Industry Association (www.siaonline.org) is the trade association for electronic security equipment manufacturers, distributors, integrators and service providers. SIA (as it is commonly known) issues Quarterly Technical Updates for its members. Updates explore timely and topical technical issues that are impacting the security industry. In the second quarter of 2005, due to the rapidly changing landscape of Federal Government security requirements, SIA's Quarterly Technical Update addressed the impact of Homeland Security Presidential Directives 5, 7, 8 and 12 on the security industry, including the fact that physical security systems, due to their computer and network elements, are now considered IT systems.

"A key concept … is that US Government automated security, access control and digital video systems are now considered Information Technology (IT) systems, and as such, all of the protections and design criteria applicable to IT systems in the Federal space will be applicable to these systems."

"Our industry has evolved significantly over the past five years. This is nothing compared to the degree of evolution that will take place over the next two to three years."

The full spectrum of security technology is being computerized, miniaturized, networked and made mobile. One result is that security technology can be affordably extended for business value outside of the security department, to support a number of business processes including quality supervision, marketing analysis, training—just to name a few. Conversely, business systems can provide security value to security processes.

One example is human resource systems providing employee hiring and termination notification, which is important to the security processes of enabling and disabling access privileges. Now that more and more security processes are becoming computer based, these business and security processes can work together automatically.

There are several major impacts of technology convergence for physical security practitioners:

- Purchasing, installing and even operating physical security systems now require knowledge beyond physical security's traditional domain.
- Because security technology can offer many non-security business benefits, and business processes can offer security benefits, security practitioners must learn about business processes outside of the security department.
- To realize all of the security and business benefits of IT-enabled security technology, especially for operating across the corporate network, the security department must now partner with the IT department.

However, there is another aspect of security technology convergence that threatens to undermine the security benefits and business benefits of putting security systems onto the corporate network. It is this: because the physical security industry had little or no knowledge of the risks and challenges inherent in large-scale networked information systems, traditional security systems were "converted" to IP-enabled systems without accounting for the security risks and networked device management challenges.

The security industry's failure to address the network security risks puts both the security systems and the corporate information systems at risk when security systems are connected to the corporate network. Failing to address the networked device management challenges creates problems for the IT department personnel who manage the corporate network.

One of the first groups to recognize and begin addressing these convergence risks is the Alliance for Enterprise Security Risk Management. AESRM (www.aesrm.org) is a coalition formed in February 2005 by three leading international security organizations: ASIS International (ASIS), Information Systems Security Association (ISSA) and ISACA. AESRM was created to address the integration of traditional and information security functions and to encourage board-level and senior executive-level attention to critical security-related issues and the need for a comprehensive approach to protect the enterprise.

"Increasingly, as a means of reducing costs, increasing efficiencies or making better use of technology investments, organizations are integrating physical security devices for access control, monitoring and process control into the IT infrastructure. This collision of two different technology worlds, each coming from a separate management approach and protection philosophy, does not always come together easily. The differences in design, functionality, implementation, maintenance and management can present conflicts, possibly resulting in a security breach involving the IT systems, the security systems or both."

Fortunately, dozens of companies have begun addressing the risks involved, and many of their lessons learned have been captured in a 32-page report by AESRM titled, Convergent Security Risks in Physical Security Systems and IT Infrastructures, downloadable from the AESRM website. The report identifies seven major security concerns based upon real-life examples of risks from organizations deploying electronic physical security systems on their corporate networks.

Beyond addressing the risks involved, there is also tremendous business value in physical security collaborating with IT to ensure that all the benefits from physical security technology are available to the organization. An added bonus is that the knowledge gained can be used to enhance the physical security of the corporate network infrastructure. It's a win-win situation for physical security and IT when organization-specific strategies are put in place to manage physical security/IT convergence.

This paper presents 10 rules that physical security departments should follow to mitigate physical security/IT technology convergence risks, help physical security properly utilize the corporate network infrastructure for security systems, and maximize the security and business benefits from physical security technology.

Strategy

Collaborations to date between physical security and IT departments have revealed five key factors that must be addressed to ensure a smooth and successful transition of physical security technology onto the corporate network. Organization-specific strategies should be developed that address these factors, taking into account organizational resources, current and future projects, technology planning, culture, and organizational priorities.

The strategies recommended below provide an effective organizational context for addressing the risks from putting your physical security systems on the corporate network.

Collaboration Team

A key concept for collaboration between the physical security and IT departments is the establishment of a *Collaboration Team*. The team needs to include individuals from the IT department who can address the IT responsibilities and functions listed below.

IT Department

- **IT Software** (product evaluation, product configuration and support)
- **IT Computer Operations** (manage server and workstation boxes)
- **Storage Management** (for external storage for video and other security data)
- **Network Transport** (IP address management, video traffic management on backbone, Quality of Service QOS)
- **IT Procurement** (purchasing)
- **Network Design** (physical and logical, including IT department standards)
- **Computer and Network Security** (including IT department standards)
- **Business Process Analysis** for business processes of interest to security, such as the employee on-boarding and off-boarding processes of Human Resources

In large organizations each of these responsibilities may be handled by a separate group. In other organization there are individuals and groups assigned more than one of these responsibilities. Many organizations also outsource some of these functions.

Notice that IT department function *IT Computer Operations* is described as computer "management" as opposed to "maintenance". This is an important distinction. Not only is one proactive and one reactive, *management* is a broader concept that includes settings, configurations, software updates, and so on in the context of a program that is intended to keep the IT infrastructure at a high level of robustness and performance. These are not just "computers"—they are the information and management systems that are used to run the business. The information and operations systems that are used to run physical security are just as critical, and require the same level of care and attention.

Why do physical security departments need to collaborate with IT about procurement? Here is a "war story" that provides an example.

For many companies this has proven to be a valuable contribution from IT. Unfortunately, some companies have learned the lesson the hard way.

For example, one company's physical security department purchased six Digital Video Recorders (DVRs) for about $48,000, to replace the tape-based VCRs they had been using. This allowed them to double the number of cameras, and extend the number of days to retain recorded video, which otherwise would have required doubling the number of VCRs and would also have tripled the manual effort involved in changing and cataloging VCR tapes. They were very happy with the initial performance of the DVRs.

Unfortunately, they did not know that the DVRs had operating system disk partitions on the same hard drives that were used to record video data. (This was the default configuration from the factory.) Thus the hard drives were overworked due to the continuous stream of video data coming in, and the resultant high level of hard drive head activity from constantly switching between operating system and video partition disk locations.

The result was that the hard drives started failing prematurely, and the systems were not even configured to display a warning message upon hard drive failure. There were other deficiencies, such as the fact that the video management software was not compatible with the anti-virus software in use at the company. This meant that the DVRs could not be placed on the corporate network. In fact, the operating system was Windows 2000 Professional, and an upgrade to Windows XP Professional would have been required to meet corporate IT standards. However, it is unlikely that the IT department would have approved the purchase of a video server system (i.e. the DVRs) that was based upon a desktop operating system.

This purchase took place in spite of the fact that the physical security department performed what it believed to be thorough due diligence on the vendor and system. They checked with other customers who had purchased the system. The customers gave a 100% satisfaction rating. They even visited customer sites, one of which had the DVRs on their corporate network. (It turned out that the other customer used a different brand of antivirus software, which actually was compatible with the video management software.) However, the other customers also started experiencing hard drive failure afterwards, because their DVR disk partitions were configured the same way at the factory.

The physical security department project team didn't realize that they needed an IT savvy person on their evaluation team, and especially for the performance of due diligence checks with other customers. Had their IT department been involved in the site visits, they would likely have discovered the poor system drive configuration and usage, and would have inquired further about the anti-virus software compatibility.

A key a convergence strategy for the physical security department is:

> *Work with the IT department to establish a collaboration team of physical security and IT department personnel who collectively encompass the full spectrum of responsibilities involved in placing physical security systems onto the corporate network.*

Another related strategy:

> *Work to understand the reason why IT departments have named these responsibilities as distinct functions. Learn what each functions role is in the big picture of keeping the corporation's information and management systems performing as planned.*

Additionally, IT infrastructure has a need for physical security. This provides an opportunity for the physical security department to be of service to IT. It also means that IT will benefit from the physical security department adopting this strategy:

> *Help the IT department get up to speed on physical security strategies, systems, procedures and terminology, enabling them to be more proactive with regard to physical security for IT infrastructure.*

Physical Security Domain Issues

There are many issues relating to physical security technology that are unfamiliar to IT departments. Of particular importance is the fact that there are aspects of physical security technology and networks that differ from what is typically found in business information systems and networks. While the differences are few, some are critical. Here are some examples.

Location of Network Connections

Physical security system components and workstations often exist in locations where IT departments would never allow computers or network connections. For example, it is not unusual to find a PC workstation for parking access control and alarm management in a parking attendant's booth. IT would not normally consider that a suitable location for a corporate network outlet or a PC, due to the obvious security considerations and the lack of typical office environmental controls.

Network Bandwidth Estimation for Video

One of the more critical differences involves the estimation of network bandwidth for security video systems. Many business networks have predictable use patterns and typical per-user allocations for storage on servers. These have been worked out over time, and can be suitably adjusted when technology improves or when the user population changes.

Most security video systems have two profiles in terms of network bandwidth—the baseline bandwidth required for continuous recording operations, and the bandwidth required for multiple operator searches of recorded video and simultaneous viewing of live video, as required for responding to or investigating a security or safety incident.

The security video network bandwidth required for a particular network segment can triple or quadruple as people from security, safety, supervision and management independently start viewing and searching video for incident response. When video is also being used for other purposes than security and security, such as manufacturing quality or process supervision, the usage can even scale up higher.

If the network bandwidth allocation for security video (i.e. how much bandwidth is made available for video data) has been misestimated or was scaled back because in practice it didn't seem to be needed, when an incident actually occurs where the bandwidth is needed, security

video performance can degrade to the point where the screen images are pixilated (only partially displayed in small square blocks) and are not usable. In other words, the video system cannot perform its intended function at the time it is needed most.

It is common IT practice to engineer a network for the worst case scenario. In other words, to build the network capacity to be able to handle the maximum bandwidth expected knowing that most of the time it will not be utilized. However, network utilization patterns of business systems can be very different from the network usage patterns of security video applications, and IT cannot rely solely on its on business systems experience.

A video system typically will run at about the same network usage 99% of the time, which is the level of usage required for recording video. The video data always takes the same path from camera to video recorders. This is fairly predictable. However, incident response and investigations is another story.

When there is a security incident, suddenly 10 or 20 people can all begin viewing live and recorded video from their desktop computers. A video protocol called *multicast* will allow a single live video data stream to be provided to multiple people over the network, so that 20 people viewing live video will only require a single video stream for each camera at any point on the network. However, if multiple people are independently searching for details by viewing recorded video, each person's search will result in an additional video data stream.

This can result in high levels of video traffic over portions of the network that do not normally carry any video traffic at all. Video data consumes a very high portion of network bandwidth compared to business applications. Sometimes in such instances the video traffic will block or slow network traffic from other systems. Sometimes there is not enough bandwidth for the video signals, and only parts of the video image can be displayed.

In most networks it doesn't matter that much where someone logs onto the network to use an business application. With video it is a different situation. Thus network planning relating to video must include examining the list of people who will be given access to video, and determining where their work takes them throughout the facilities. Each portion of the network that may be required to carry video information must be taken into account.

Video Storage Performance

Similarly for video storage, there are two performance situations. The first situation is during normal usage where the storage system is continuously recording but not serving up any recorded video streams for viewing. The second situation is incident response, where multiple people are viewing recorded video.

During a high usage incident, not only must the recording continue, but now 5, 10 or 20 operators must be served, each of whom may be accessing multiple camera streams in addition to the live stream. It is not uncommon for video system performance to degrade if the performance of the storage system is not up to the task. This is one reason why many DVR

manufacturers limit the number of operators who can simultaneously access video from the DVR.

Similarly, storage requirements can change dramatically based upon any number of factors. If video is being recorded for 15 days because security incidents are reported immediately or within a day of their occurrence, what happens if an important asset is found missing, and no one has entered its storage room for 3 weeks? Security can conclude that 30 or 45 days of video storage is required, doubling or tripling the storage requirement. Legal or audit requirements can also impact the term of storage. Although outside the technical scope of this paper, other factors can impact the storage requirements, such as recording rate (images per second) and resolution of camera video images (640 x 480 or 320 x 240, for example).

Helping IT with Security-Specific Issues

These are some of the ways that security video requirements are very dissimilar to video-on-demand or video conferencing requirements, the kind of video systems that IT departments are familiar with.

That means special steps are needed to collaborate with IT to determine what the network requirements will be for the security systems, especially video systems. Access control systems don't require much network bandwidth; video systems do. Your systems integrator is part of your team and should work with you in collaborating with IT about video network requirements. Your integrator can obtain and provide you with the information you need to calculate network bandwidth required for camera live data streams, and for recorded data streams being played back. This will depend on the size of the camera images, the recording rate in images per second, and other factors.

To develop the network bandwidth requirements for the continuous recording video profile, provide IT with the locations of all new and existing cameras and their recording equipment, or with the "first pass" design locations for equipment not in place. If some cameras are analog cameras that will have their signals converted to digital signals, provide the locations for the video converters (this could be at the camera or in an equipment closet where video signal cables are routed).

Many camera and video system vendors provide "average" camera network bandwidth requirements. That can lead to a situation where during maximum usage there is insufficient bandwidth available. Use worst-case calculations in a reasonable way.

To develop the network bandwidth requirements for the investigations and incident response profile requires providing specific information to IT as to how the systems are used. How to go about this—not just for video but for any aspect of collaboration with IT about network use or integrations with business systems (such as a Human Resources system)—is explained below.

An important strategy for video systems is:

> *Do not use "average" camera requirements to calculate bandwidth. Use worst-case calculations based upon realistic scenarios for maximum capacity requirements. Explain to IT that the maximum network and system capacities will be seldom used, but when required will be critically needed.*

Information for the IT Department

There are two types of information that you must provide to your IT collaboration partners: information on security processes, and information on how the security technology is used to support those processes. This information should be captured in *scenarios* and *use cases*. It is important to know that the terms *scenario* and *use case* are terms commonly used in software development work, and sometimes the terms are used interchangeably. *In this paper the terms have very specific definitions which are definitely not interchangeable, and it is important that these exact definitions are provided to the IT personnel collaborating with the physical security personnel.*

> A *scenario* is a brief description of a security event or of how a security operations task is performed. A scenario describes the event or activity in technology-free language. It should capture the overall *process* that one or more security personnel must perform, and which the technology supports though one or more features or capabilities.

Scenarios are especially important for capturing the processes that must be integrated between security operations workflow and workflow in other departments. For example Human Resources hiring and termination processes should trigger the assignment and cancellation of security access privileges. Identifying the points of integration in each business process leads to the related systems processes and to the identification of the correct points of system integration. It also helps to ensure that the business processes actions are sufficient to accomplish the intended result.

For example, one company integrated their physical access control system with the corporate directory (which was implemented using Microsoft Active Directory), in order to capture employee terminations as soon as they happened. They were shown this approach by a sister company who had implemented this particular integration. When they integrated it in their own company it didn't work. People were terminated in the HR software, but not in the access control system. It turned out that the HR software did not automatically remove people from the Active Directory system until after their final paycheck was issued—sometimes two weeks after termination. No one had examined the business processes involved, because they didn't realize that the purpose of the systems integration was to *integrate the business processes*. This situation was easily remedied by incorporating termination information in the directory records, which then was used to trigger the instant cancellation of security access privileges.

Develop a list of the scenarios for the key aspects of normal operations and incident response that will require security system information be sent over the corporate network. For each scenario developed, develop a *use case* for the security system elements involved in the event management response or the performance of the operations task.

> A *use case* describes the interaction between a system operator and the system itself, represented as a sequence of simple steps. The use case information should include the network data flows involved (i.e. what information is sent across the network from one computer to another or between a field device such as a camera and a computer).

For video, the use case information along with video system technical information will be used to determine how much network bandwidth is required. Your systems integrator and/or your video system vendor should help with the network bandwidth calculations.

Thus two good convergence strategies for the physical security department are:

> *Use security scenarios to develop use cases, and work with your systems integrator to collaborate with IT in developing network bandwidth requirements from them.*
>
> *As part of that requirements development, work out the network data flows for video traffic. There is one set of data flow paths for recording, and another set for security, safety operations, supervisory and management personnel to view video. Determine all the locations in each facility where video may be viewed for any purpose.*

IT Domain Issues

For several years security publications in both the physical and IT domains have been publishing articles about the "convergence of physical security and IT security". However, it is not only IT security but the full spectrum of information technology and IT operations that is converging with physical security systems.

In particular, there are IT issues involved in placing technology onto the corporate network that are new to physical security personnel. For example, IT has developed standards for ensuring that its networks and computing systems are robust, secure and manageable. It is a growing IT practice to include redundant paths in network design, to allow the network to be self-healing. These standards should be applied to physical security systems being placed on the corporate network. These systems also need to be robust, secure and manageable, don't they? Where information about these IT standards is not readily available, physical security personnel should request it.

Evidence that the application of IT standards to physical security systems is a trend that has arrived comes from the physical security industry's largest customer, the U.S. Federal government, who in essence declared that physical security systems are IT systems.

The Security Industry Association (www.siaonline.org) is the trade association for electronic security equipment manufacturers, distributors, integrators and service providers. SIA (as it is commonly known) issues Quarterly Technical Updates for its members. Updates explore timely and topical technical issues that are impacting the security industry. In the second quarter of 2005, due to the rapidly changing landscape of Federal Government security requirements, SIA's Quarterly Technical Update addressed the impact of Homeland Security Presidential Directives 5, 7, 8 and 12 on the security industry, including the fact that physical security systems, due to their computer and network elements, are now considered IT systems.

"A key concept … is that US Government automated security, access control and digital video systems are now considered Information Technology (IT) systems, and as such, all of the protections and design criteria applicable to IT systems in the Federal space will be applicable to these systems."

"Our industry has evolved significantly over the past five years. This is nothing compared to the degree of evolution that will take place over the next two to three years."

The evolution described by SIA is one whose primary element is the continued incorporation of information technology and its related technology standards. In the corporate environment not only do IT standards apply, but also *many aspects of how IT does business are applicable*. Technology evaluation, planning, procurement, deployment, operations and maintenance all are parts of the picture that physical security departments need to know about. Service level agreements, network Quality of Service, patch management (keeping operating systems updated or "patched") and many other important aspects of managing and maintaining systems are new to physical security personnel, and are now critically important to their systems.

Thus one sound strategy for physical security departments is:

> *Get educated by the IT department on how IT does business, and how the full lifecycle management process for IT systems and equipment is addressed.*

That is not as easy as it may sound, because IT personnel are used to IT terminology and concepts and include them in everyday discussions. Physical security personnel are often completely unfamiliar with many of the IT topics that apply to their systems, and can easily get lost in what IT considers to be basic conversation.

Thus another strategy for physical departments to consider, if there are no IT-savvy personnel in physical security already, is this one:

> *Don't be completely dependent upon IT for education on IT issues. Designate at least one physical security team member (an employee, consultant or contractor) be designated to become "IT-savvy", and collaborate with IT to develop a list of education topics relevant to the physical security systems moving onto the corporate network.*

Collaboration with IT should consist of more than simply having meetings. Many corporations use *mentoring* as means to foster knowledge sharing and skill development.

> ***Mentorship*** refers to a developmental relationship between a more experienced **mentor** and a less experienced partner referred to as a **mentee** or **protégé** – as person guided and protected by a more prominent person. –Wikipedia

It is in the interests of both departments for IT to establish two-way mentoring. While it is true that physical security requires a larger flow of information and education from IT than IT does from physical security, it is important to consider the critical importance of physical security to IT. Many information losses involve someone walking out the door with a laptop or other device containing data. Most IT infrastructures do not have sufficient physical security applied to them, and for those that do the measures are more ad hoc than they are strategic. Neither department should underestimate the value of physical security information to IT.

Physical security has a longer history of investigations and incident response than IT, and has very robust processes for such work. This is another are where IT can benefit by leaning from physical security practices.

Another difficulty with information exchange in general is that we tend to take for granted a lot of what we know. Some knowledge is so familiar they we never even think about it—we just do what we need to do almost automatically. Thus it can be hard in a meeting setting to call up basic information for discussion. It's just not in the forefront of anyone's mind. Another difficulty with knowledge sharing is that we don't know what we don't know, so how could we specifically ask about it?

This is where the practice of *project shadowing* really helps. A *shadow* is a person assigned to a project team for the purpose of observing and learning. A common reaction from the initial shadowing experience is: "Wow—there is a lot more to this than we knew about!" Shadowing provides insight based upon real-world situations and experiences.

Follow this valuable strategy to enhance the speed and effectiveness of knowledge transfer:

Use mentoring and project shadowing to help facilitate the transfer of knowledge and skill.

When using mentoring and project shadowing, keep in mind the phenomenon described in the section titled, "Separation by a Common Language" on page 18.

Until you have an IT-savvy person in physical security (i.e. while you are still heavily dependent upon IT), be considerate of your IT department allies and keep in mind that they usually have their own tasks, deadlines and priorities assigned to them. Try to give them as much notice as possible for meetings or collaborative activities, including providing meeting agendas in advance, to facilitate smooth and effective IT and physical security collaboration.

Non-Security Benefits to the Organization

Using physical access control systems to provide payroll time and attendance records began to be popular back in the early 1980s. That was the first non-security application for electronic physical security systems. A current and growing trend is the use of security video technology for non-security business purposes.

Example applications of business value are:

- retail marketing analysis of customer behavior in response to store layout designs or merchandise display changes
- employee training
- manufacturing quality and process control supervision

Such applications are of particular interest because they significantly increase the ROI from security video technology, and can bring additional budget dollars to the table from non-security stakeholders. Such applications are of technical interest to IT departments because they mean that security technology must be extended even further across your corporate network. Implementing such IT-enabled applications also means that IT is providing added business value, so it is prudent to for IT departments to be proactive in the planning and deployment of these applications. Collaborating around non-security applications of security technology will involve sharing information that previously the physical security department has not shared.

Here is a strategy for physical security departments who can extend the use of security technology for non-security business benefits:

Be attentive for opportunities to apply physical security technology for business purposes, and document the related business cases to share with IT. When IT understands how helping physical security adds value to the business, it is easier for them to assign resources to the collaboration.

Roles and Responsibilities

When it comes to putting physical security systems onto the corporate network, there are issues new to both the physical security and IT domains. Thus there is often a lack of clarity about who should be doing what. There is a natural tendency to focus on the technology issues, as opposed to the people and process aspects. Proper attention to the people and process aspects is what enables a smooth technology transition.

The physical security personnel involved in their security technology projects will benefit from learning about the IT department processes involved in deploying networked systems and devices. Additionally, getting the physical security personnel up to speed on those processes will help to eliminate unnecessary burdens on the IT personnel. Once the processes are understood in both domains, roles and responsibilities can be assigned appropriately and effectively.

This strategy takes away a lot of the pain involved in migrating physical security systems onto the corporate network:

> *See that the physical security personnel involved in putting technology onto the corporate network get educated on the IT processes for deploying networked systems and devices. Establish a cross-functional team with roles and responsibilities assigned appropriately for IT department and physical security department team members.*

Planning and Execution

An important element of migrating physical security systems onto your corporate network is the recognition of the two-phase aspect of the transition. The first phrase is *initial migration*, which involves getting existing or new systems onto the network. The second phase is *management and maintenance* for the computer and network elements (often called "Day-2 support" by IT personnel).

It is important to define the *initial migration* phase with a beginning, middle and end for several reasons. It has been common for physical security and IT personnel to simply "fall into" the work without realizing the full scope of the initial effort. Before long the personnel involved are overwhelmed by the scope of the effort, especially when they have other responsibilities. The ad-hoc education of the physical security department personnel is very time-consuming, but such education is absolutely required. Thus work and collaboration that should be captured in an initial phase (very early in the project) is instead spread out on an as-needed basis, often in response to problems that arise because such work was not performed earlier.

As a result of such situations, early convergence projects have given both IT and physical a bad impression of convergence.

Without clearly defining these phases, IT and physical security departments can get seriously out of sync on the technology deployment. When a physical security project for technology deployment has been defined without accounting for the critical IT elements (as has often been case), the IT personnel end up as "adjuncts" to the project, with little control or influence, when in fact they should have had initial and continuing participation in its planning.

Due to schedule pressure and security needs, it is not uncommon for the physical security systems to be implemented with the IT security and device management aspects unaddressed. This makes for an operationally awkward situation in which the physical security project is "finished" but the IT concerns are only partially addressed (only to the minimum extent necessary to get the systems working and performing their functions).

Participants in such projects must realize that prior to the first time physical security technology is placed on the corporate network a lot of work must be done up front which will, thereafter, be applicable to all physical security technology projects.

Calling this work an "initial migration phase" is an accurate characterization of the key aspects of this work. It is the first time it is being performed. Security systems are "migrating" from one electronic "location" (as standalone implementations) to another electronic location (residing on your corporate network). Just as moving a business from one location to another is a complicated and involved process, moving security systems from their current independent status to residence on the corporate network is a complicated and involved process—but is completely manageable and can be a smooth transition if approached with proper planning and execution.

When the "initial migration" phase is over, it is immediately followed by the management and maintenance phase. Networks, information systems and businesses are dynamic. This includes enterprise physical security systems and the corporate networks they reside on, especially when such systems are integrated with business systems outside of the physical security department.

This requires a change in thinking on the part of physical security personnel, who are used to a much simpler two step deployment process: *install then operate*. Previous generations of systems required mostly physical maintenance, so things like operating system patching, software updates, and network upgrades are unfamiliar to most physical security departments. In the traditional model the physical security systems integrator did the maintenance and often the management of the system; now that model must be shifted to include support of IT resources to do some or many of the elements previously done by the security integrator.

Not only do these aspects of operating on the corporate network require education for the physical security personnel—they must be incorporated into their technology planning.

Thus another important strategy for physical security departments is:

> *Work with IT to identify what is involved in the initial migration phase and the management and maintenance phase, and ensure that these phases are incorporated into the physical security technology planning.*

An additional strategy worth adopting is:

> *Include both an executive sponsor and a project manager in each initiative. These roles should extend into system lifecycle planning as well.*

System Lifecycle Planning

Most physical security system providers don't yet apply technology lifecycle planning to their technology projects, and of course neither do most physical security departments. This aspect of project planning is important and involves considerations in both the IT and physical security domains. It has an impact on the information that you need to obtain regarding the corporate network.

For example, one company upgraded all of its older video-compatible network switches to newer ones as they approached their support end of life, but did not purchase the video compatibility options for the new switches. The new switches are upgradeable and so they decided to pay for the video features if and when they deployed video conferencing or some other technology that required it.

In the mean time the physical security department had earlier asked what kind of network switches were on the network, and IT answered. But the future upgrade was not discussed. The physical security department planned and obtained budget approval for a new network-based video surveillance system, but did not include the cost of upgrading the network for the network switch video option upgrades. IT upgraded the network switches as planned. Later when the next fiscal year's budget arrived, physical security began its project, only to collide with the fact that key portions of the corporate network would not support transport of the video camera data streams. Needless to say some serious finger-pointing occurred, and a senior manager rightly criticized both the physical security and IT departments for not collaborating sufficiently.

IT can help the physical security department adopt technology lifecycle planning for the physical security systems to the benefit of both departments.

Level of Service

In order to fully establish the roles and responsibilities for a cross-functional project for physical security technology, the level of service that will be provided by the IT department, for both the initial migration and the management and maintenance phases, must be established as early as

it can be in the project. This is because IT department resources are almost always fully allocated, and are generally not available on a moment's notice except for help desk issues.

Early convergence often moved forward without a sufficient scope for the IT elements in their advance planning, and collided with unaddressed IT requirements as they moved forward. IT departments appeared uncooperative when they couldn't provide support at the instant it was requested. Or worse, trying to help out, IT provided the most available person, who was typically unfamiliar with the physical security systems and could only converse about the IT aspects at a much too technical level for the physical security personnel.

This situation was commonly reported to management as the project having "technical problems" or "personnel problems", when in fact it was actually a project planning issue. Management efforts were often directed at solving the wrong problem. This typically resulted in unusual solutions being applied, which often remained troublesome *because they were not a part of the usual IT processes.*

One of the usual IT approaches to providing services is a Service Level Agreement (SLA), which specifies exactly what services will be provided, by whom, and under what conditions. Although IT department has SLAs with outside firms that incorporate some very technical language, physical security system support does not require lots of technical specifications in the SLAs.

"We have found that Service Level Agreements (SLAs) between IT and physical security have been very workable in supporting our physical security technology."

Deon Chatterton
Senior Manager - Integrated Building and Risk Technologies
Cisco Systems, Inc.

Although it is time-consuming to work out SLAs for the first time to support physical security system projects, it is a fraction of the time that will have to be expended if the issues involved are not worked out in advance. Standard business processes for resource allocations can be applied when SLAs are in use.

Thus an important strategy is:

> *Develop SLAs for the initial migration and the management and maintenance phases for moving physical security technology onto the corporate network.*

There is one caution; many physical security system components are not designed with the High Availability (HA) elements, such as redundant power supplies, dual communication paths, and hot standby systems that IT requires to enable IT to provide the quick SLA response times

in servicing the system. This can often be disappointing to the security manager, who feels that the security system should get the same immediate response results from IT that IT systems get.

Security system data is critical data, and deserves the same High Availability designs that are applied to IT systems and networks, both to establish an appropriate level of system robustness, and to enable the appropriate level of service by IT. Video storage in particular should be considered in this regard.

Thus an additional important strategy is:

> *Learn about the High Availability design approaches that IT uses for networks and systems, and incorporate them as appropriate in your physical security systems designs.*

Separation by a Common Language

A unique challenge to physical security and IT collaboration is the terminology used in each domain. While the concepts are basically the same for most terms, a single term can refer to different items in each domain. For example, “IP” means “Intellectual Property” to corporate security, but “Internet Protocol” to IT security folks. For example, a physical security manager might say, "We have removed all the IP from the corporate network," meaning that all critical intellectual property documents have been removed from computers connected to the corporate network. This would eliminate the threat of documents being accessed by a hacker on an internal or Internet network connection. That sentence would sound absurd to IT personnel, because network communications are based on IP messaging!

What happens when these terms come into play is that discussions go along fine until a term is utilized. Then the participants who have another definition than the speaker start developing strange ideas about what is being said. If it happens too much, one side or the other gets into a “mental fog”, and can’t really track with the rest of the discussion. Parts of major initiatives have gone off the rails over this specific phenomenon. Table 1 provides some examples of the terminology differences. Once aware of this phenomenon, participants can recognize when the definition difference has come up and address it on the spot.

Table 1. Examples of Terminology Differences

Term	Physical Security	IT
IP	Intellectual Property	Internet Protocol
Credentials	ID Badge; Passport	Digital Certificate
Key	Key for physical lock	Encryption key
Perimeter	Fence line or exterior building walls	Network connection to outside or public networks
Intrusion detection	Door/window alarm system	Computer & network hacker detection
Directory	Lobby Building Directory	Electronic Network Directory
Security Logs	Reception sign-in sheets; Journal of security officer shift notes	Lists of access attempts to computers and networks

Term	Physical Security	IT
Revocation	Canceling and retrieving a security ID badge	Canceling a digital certificate
Signature	Written signature	Digital signature

On the other hand, there are a lot of common concepts between physical security and IT domains—after all, they both deal with security—and so Table 2 provide examples of the commonalities between the two domains in terms of security concepts.

Table 2. Examples of Common Concepts

Security Component	Physical	IT
Perimeter Barriers	• Walls and fences	• Firewalls
Access Control	• Locks & Keys • Keypad Pin Codes • Biometrics • Access Cards	• Password Codes • Biometrics • Smart Cards
Alarms	• Intrusion Detection: Motion Detectors, Glass Breaks, Door Contacts, Fence or Perimeter Intrusion Detection Systems (IDS)	• Intrusion Detection: Network Intrusion Detection Systems (IDS)
Investigative Tools	• Interviews • Collection of Evidence (Forensic Physical Science) • Evidence Analysis • Identify Cause or Suspect	• Interviews • Collection of Evidence (Computer Forensics) • Evidence Analysis • Identify Cause or Suspect (Network Forensics)
Notice i.e. "No Trespassing"	• Physical Signs ("Keep Out")	• Computer Messages ("Keep Out") • Acceptable Use Agreements
Security Resources	• Contract Security Officers • 911 – Law Enforcement Response • Community Law Enforcement Programs	• Consultants • High Tech Crime Units • FBI Infraguard Program • Carnegie Mellon/CERT
Risk Assessment or Security Surveys	• Inspection • Threat and Vulnerability Analysis • Testing	• System Configuration Inspection • Threat and Vulnerability Analysis • Attack and Penetration Testing
Awareness and Training	• Bomb Threat Training • Workplace Violence Training • Security Awareness Training	• Incident Response Training • Protection of Information Training • Security Awareness Training

Additionally, some terms that are in common use are not fully understood even by some of the people using them. For example, the term *bandwidth* is commonly used to refer to how busy a person is ("I don't have the bandwidth for that today"). People can also get all kinds of strange ideas when they try to take definitions from the context of the sentence. For example, "Look at the screen, you can see there isn't enough bandwidth," can give someone the idea that the width of the visual image on the screen is what is meant by bandwidth, when the person was talking about the display of available network bandwidth. This has actually happened. And

there have been people who think that CCTV refers to a cable television station like MTV rather than a camera surveillance system—Closed Circuit TV.

This is why a strategy is needed to guard against miscommunication:

> *Establish, publish and follow meeting guidelines for cross-functional communication that account for the educational differences among the participants. Also apply them to your personal communications.*

An example meeting guideline is included as Appendix A to this document.

With practical strategies like these in place, you have an excellent chance of success in moving your physical security systems onto the corporate network, and helping ensure that the business receives the full potential value of the systems.

Putting Your Systems on the Corporate Network

The ten rules below provide effective ways to address the key issues involved in putting physical security technology onto the corporate network. Beyond security risks, there are other risks involved because the information technologies being incorporated into physical security's systems are new to them. There are risks involved in network and system design, technology evaluation, purchasing, deployment and maintenance that must be addressed to ensure that your organization receives its money's worth and that the systems start up and continue to operate as intended.

In 2003 Cisco's IT department launched a project to help its physical security department "Go IT" the right way. This was prompted by an incident where Cisco's physical security group lost the majority of its global video surveillance capability due to the Nimda virus infecting the security department's newly deployed Digital Video Recorders. (To read the case study, download this document from the *Best Practices for protecting IP-based Security Systems* website: http://www.cisco.com/web/about/ciscoitatwork/security/cctv_on_ip_network.html.)

If this kind of situation can happen to Cisco, it can happen to your company. Your physical security department needs you, the IT department.

Your attention to these issues below will also help ensure that the physical security technology purchased and deployed provides the security functions it is supposed to provide under all anticipated conditions, and that the people and critical assets of your organization are protected as planned. This is both a security responsibility and a fiscal responsibility.

One: Put Someone in Charge

You must designate someone from the physical security department to lead the collaboration effort with IT. This person should not be a project manager for the migration of physical security systems onto the corporate network, nor should it be the executive sponsor. It can be

the person overall responsible for the migration. With regard to the migration, this person's sole job should be the orchestration of the collaboration between physical security and IT. It is a critically important function, so don't underrate it.

Two: Develop Your Business Case

The most important thing that you can do to get your physical security systems onto the corporate network is to develop the business case for doing so. That is the first action of the person responsible for physical security and IT migration. The business case should not be a "generic" pitch assembled from trade magazines and other literature. It should be specifically based upon the needs and opportunities within your own organization.

Three: Get Your System Documentation Current

When they do exist, most security system design documentation and engineering drawings are out of date. In contrast, most IT departments have their design documentation and engineering drawings current. Don't be surprised if your IT department considers one of their own drawings out of date because it doesn't incorporate a change that was made only a few weeks ago. Things move fast in the IT world, and one of the reasons they can is the attention paid to critical documentation.

You will win respect from IT if your documentation is up to date. If it is not, they will consider you unprofessional, and they won't be wrong. If you have to spend money to get a professional engineering services firm to help you, make it happen.

If you can't get your documentation up do date, how will you ever execute all the other work that you need to do?

Four: Put Your Collaboration Team in Place

Once your documentation is updated, figure out who the IT manager or executive is you should first consult, and get your business case to him or her. Find out who in IT is responsible for the IT functions listed on page 4 of this paper, and build an appropriate team. If the IT manager or executive is not the appropriate person to be the executive sponsor, have them recommend a candidate. Executive sponsors have been proven to be critical to the success of convergence initiatives.

Five: Inform and Educate Your Systems Integrator and Key Vendors

Your system integrator and key vendors are important partners in your technology deployments. Put this paper into their hands, and use it as a basis for collaborating with them about getting your systems onto the corporate network. Integrators and vendors are adding more IT-savvy people to their organizations every day. They can help you make the transition to being an IT-savvy physical security department.

Six: Identify the Applicable IT Standards and Requirements

There will be a number of IT standards that apply to physical security system design in terms of computer, software and network components. Often these have a higher retail price than what the physical security department is used to spending. On the other hand, IT often has excellent purchasing arrangements, and you can leverage their buying power to advantage.

Remember the tremendous benefit you are getting from IT standards. These are hardware and software solutions that have been proven to be robust, manageable, and have high performance. They are just what you need.

Seven: Learn From the Way IT Approaches Technology Projects

You will do well to learn from their approaches to project planning. Most IT departments have executed several enterprise-wide technology projects. They have learned a lot the hard way. You can benefit from their trials by fire.

Eight: Be Open to IT Advice, and Willing to Share With IT

Don't get defensive if you get criticized or if something about physical security operations evokes a surprising reaction from IT. Get a high tolerance for "nerdiness". Learn from such experiences. In spite of the temptation, don't justify or be argumentative. That will only lower your status in the eyes of IT. Also, be willing to share your knowledge with IT personnel. Besides being good for your organization, it will help strengthen the relationship between physical security and IT.

Nine: Get Up to Speed on Test Planning and Execution

The testing of physical security systems can be very involved depending upon the sophistication of the security technology being deployed. There are several unique aspects to physical security system testing, in contrast to testing business information systems:

- Selected features are tested, instead of all the features.
- Scenario-based testing is performed for both normal operations and for security incident response.
- The system "goes live" before the final acceptance testing is complete
- End user training is required before final testing, not after, because the system will be put into full use as part of the final test phase.
- Personnel from the different work shifts (day, afternoon, night, weekend, etc.) should participate in the testing.
- To make best use of new systems and new technology, security processes and procedures may need to change, and new procedures may need to be developed. The related organizational functions must also be tested and/or practiced before the system can undergo final acceptance testing

It is neither practical nor desirable to test all the features of a physical security system. In fact, some features will be mutually exclusive. What is important is to test the features that are intended to be used, *in the same way that they are intended to be used*.

Remember the *scenarios* and *use cases* described earlier in this paper? They should be used again as the basis for testing.

For the final acceptance test, the system must be operated continuously for a minimum period of 30 days. That is the period of time that it generally takes to exercise the system under its various conditions of use, and to use all of the features that are intended for use. It is also the security industry's generally agreed upon time period required to demonstrate system reliability. For this final acceptance test, the system has "gone live" and is actually being used to protect facilities and personnel, prior to full acceptance! This is one reason why system acceptance testing is a critical activity. Many IT departments tests critical systems for 30 to 90 days, and if the IT personnel suggest a longer test period, consider their recommendation.

Note that for video systems, a test period longer than 30 days may be needed to fully test all functions. Video systems are configured to store data for a certain period of time, or up to a certain storage capacity, and then start writing new video data over the oldest data. For such systems the testing should extend to the point where the maximum stored video retention period is reached, and older video data starts being overwritten with new video data.

For all of the reasons listed above, you should require a complete written test plan at least two weeks before testing is scheduled to begin. Expect that the first draft of the acceptance test will not be sufficiently developed, and expect to collaborate on its completion. Most security system providers omit network related testing, such as full testing of new network segments installed, and verification that the system's bandwidth use is as designed.

The security systems integrator is an important part of the test team. Regardless of who develops the test plan (integrator, physical security or IT) include the systems integrator early in the test planning effort.

A full description of security system testing is beyond the scope of this paper. The best approach is to engage someone for the project who is experienced in physical security system acceptance testing.

The final recommendation with regard to testing is: be prepared to hold your ground and insist on a formal test plan. An actual project experience illustrates why. On a recent $9 million security systems project, the system provider was able to talk the customer's procurement office into canceling the testing requirement, three separate times during the project! If you suspect that was because the system provider was not up to the task, you are correct. Testing was reinstated each time at the insistence of the physical security and IT project managers, and as a result the project was only one year late, not two years—as it would have been without the

testing program. Remember that IT will be on your side about this. Use a little of their clout if you need to.

Ten: Document and Share Your Success

Your physical security colleagues will benefit tremendously from learning about how you accomplished “Going IT”. In addition to presenting at security association chapter meetings and security conferences, consider the trade associations to which your company belongs. If your company won’t spring for the travel expenses, perhaps one of your vendors will if you can highlight how they helped you.

Set an example by sharing your knowledge. As others do the same you will learn even more.

Conclusion

There is tremendous value added to the business when IT departments and physical security departments collaborate in moving the IP-enabled physical security systems onto the corporate network. With sound strategies and an understanding of the challenges involved, that migration can proceed smoothly with significant benefits to both departments.

Acknowledgements

The author's thanks go to the following individuals who improved to this paper by their review efforts, suggestions and additional material. Robert Sayle also acted as editor for the paper.

Robert Sayle
Systems Engineer - CCIE, CISSP, CHSP
Cisco Systems, Inc.

Deon Chatterton
Senior Manager - Integrated Building and Risk Technologies
Cisco Systems, Inc.

Kelly J. "KJ" Kuchta, CPP, CFE
President
Forensics Consulting Solutions, L.L.C.

Intransa

A special acknowledgement goes to Intransa, the VideoAppliance Company®, who sponsored the research for this paper and its companion paper for IT departments, "Twelve Ways to Address the Risks from Putting Physical Security Systems on Your Corporate Network." Intransa is the industry's leading provider of green, affordable and reliable video surveillance platforms. For more information, please visit Intransa anytime at www.intransa.com.

About Ray Bernard

Ray Bernard, a security industry analyst, journalist and author is also President of Ray Bernard Consulting Services (www.go-rbcs.com), a security management and technology consulting firm. Bernard has provided pivotal direction and advice to the security industry (manufacturers and service providers) and to the security profession (security management) for over 24 years. Bernard was named as one of security's *Top 10 Movers and Shakers of 2006* by *Security Technology & Design* magazine.

Bernard is also founder and publisher of *The Security Minute* electronic newsletter (www.TheSecurityMinute.com), the first newsletter for security practitioners and management security stakeholders—the people involved in making or approving security decisions, policies, plans and expenditures.

Bernard writes a monthly column called 'Convergence Q&A" for *Security Technology Executive* magazine, as well as six feature articles per year around key convergence issues. Bernard is also a contributing editor to *The Encyclopedia of Security Management*, 2nd Edition, for its security convergence subject entries.

Bernard is Board Certified as a Physical Security Professional (PSP) by ASIS International; Board Certified in Homeland Security (Level III) by the American College of Forensic Examiners International (ACFEI); active council member of ASIS IT Security Council and the ASIS Physical Security Council. Bernard is also a supporting member of the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), and the IEEE Computer Society.

About the Bp.IP Initiative

The mission of the Bp.IP Initiative is to help achieve IP-based physical security technology deployments that are:

- Secure
- Technically Sound
- Cost-Optimized

Secure systems are at low risk of compromise and can be maintained at a low risk profile.

Technically Sound systems are not prone to failure due to technical weaknesses. This applies to all electronic security technology, from legacy to leading edge systems.

Cost-Optimized systems are well-documented as well as well-designed, so that the costs to design, install, commission, operationalize, maintain and evolved the systems provide an outstanding Total Cost of Ownership picture.

You only "get what you pay for" if you follow best practices for deploying IP-based systems. Otherwise you spend more and get less.

The **Bp.IP initiative** is an ongoing effort that continually assesses the state of the physical security industry and provides best practice guidance based upon the current state and trends of technology and what constitutes sound deployment practice.

For more information, please visit **Bp.IP initiative** at www.BPforIP.com.

Appendix A

Physical Security and IT Meeting Guidelines

Here are some guidelines that can be applied to all meetings, but which are especially important for meetings where both Physical Security and IT topics will be discussed:

- **List the topics to be covered.** At the start of the meeting, list the various knowledge domains that will be covered in the meeting. Ask for a show of hands if a domain is not a primary subject of expertise. If any hands go up, emphasize the importance of not going past any point that isn't completely understood. Explain that the success of the meeting and the follow up actions is important enough to take the time to clear up any questions.

- **Schedule attendance for mixed agenda meetings.** Try scheduling the topics so that people won't be unnecessarily subjected to domain-specific discussions. Someone from accounting should not be expected to sit through a lengthy technical discussion. Skip the technical discussion and give a plain English summary, or schedule the technical discussions first with a limited group and bring others into the meeting at a later point.

- **Specify who can answer questions.** Sometimes people can think they understand something, to find later that they don't. By the conclusion of any meeting, make sure you have identified who should be contacted about questions specific to each topic of discussion.

- **Check for questions.** At the conclusion of each topic, not just at the end of the meeting, check for questions. If being considerate of questions is something new in your organization or department, you may have to overcome the reluctance of some people to ask questions.

- **Clearly define terms.** Be sure to define each topic term clearly when you first use it, and make it obvious when you are switching topics. You should have definitions written out in advance, that use plain language and avoid references to other words that would not be known to the meeting attendees.

- **Be brave.** Ask a question when you don't understand. Often others will have the same question. Lead by asking. Others will follow your example.

- **Be considerate.** Be patient in helping someone else understand what you are saying. It's your responsibility as the person speaking to make sure that you get your message across. This means you have to take the steps necessary to clearly explain what you are saying at the level of the listener. Remember what Einstein said: "If you can't explain it to a six year old, you don't understand it well enough yourself."