BP.IP™ Best Practices for IP-Based Systems

Twelve Ways to Address the Risks from Putting Physical Security Systems on Your Corporate Network

How IT Departments Can Support the Benefits of Physical Security's "Going IT"

by Ray Bernard

v 1.6

Table of Contents

Introduction 1

Strategy 2

IT Domain Issues 2

Physical Security Domain Issues 4

Non-Security Benefits to Your Organization 6

Roles and Responsibilities 7

Planning and Execution 7

Level of Service 9

Separation by a Common Language 10

Addressing the Risks 12

One: Require Computer and Network Security 12

Two: Require All Networked Systems and Devices to Meet IT Standards 14

Three: Direct or Assist in the Network Design and Planning 14

Four: Collaborate on Technology Lifecycle Planning 15

Five: Provide Technology Evaluation for the Software and Hardware IT Elements of the Security Systems 15

Six: Plan or Help Plan the Systems Deployment 16

Seven: Require the Written Planning and Execution of a Complete Acceptance Test Plan 16

Eight: Ensure That System Design and Deployment Meets Corporate Privacy and Data Security Compliance Requirements 18

Nine: Provide Systems Maintenance Under an IT Department SLA 18

Ten: Implement Authorization, Accountability and Auditability Controls 18

Eleven: Support Unified Security Initiatives such as Role Based Access Control and the Use of a Single Security Smart Card for both Physical and Logical Security 19

Twelve: Treat the Physical Security Systems as Other Corporate Critical Data Systems Are Treated 19

Conclusion 19

Acknowledgements 20

About Ray Bernard 21

About the Bp.IP Initiative 21

Introduction

IT executives and managers in many organizations are being confronted by a new situation: physical security systems and equipment are migrating onto the corporate network, often with little or no consultation or advance warning to IT. The trend is the result of the convergence of information technology (computers, databases, wired and wireless networks, and embedded computing) into traditionally standalone electronic physical security systems and equipment. Card and keypad based access control systems and video surveillance systems, for example, now are IP-enabled and utilize Ethernet network communications.

One of the first groups to recognize and begin addressing the risks of this convergence trend is the Alliance for Enterprise Security 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 (formerly known as the Information Systems Audit and Control Association). AESRM was created to address the integration of traditional and information security functions and to encourage board 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."

The Alliance for Enterprise Security Risk Management℠

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 IT collaborating with physical security to ensure that all the benefits from physical security technology are available to the organization. An added bonus is that IT can benefit by collaborating to enhance the physical security of your 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's "Going IT".

This paper presents twelve specific ways that IT departments can 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 on the following pages provide an effective organizational context for addressing the risks from putting physical security systems on your corporate network.

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 your 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. These standards apply to physical security systems being placed on your corporate network. Often these standards are not accessible by the physical security technology personnel.

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 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 IT departments is:

> *Educate the Physical Security department on how IT does business, and on IT's approach to full lifecycle management of IT systems and equipment.*

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. The physical security personnel are completely unfamiliar with most 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 IT departments to consider, if there are no IT-savvy personnel in physical security already, is this one:

> *Shift the burden of educating physical security personnel on IT issues over to the physical security department, over time. Require that at least one physical security team member (an employee, consultant or contractor) be designated to become "IT-savvy", and recommend a list of education topics relevant to the physical security systems moving onto the corporate network.*

Conversely, IT departments should also adopt this strategy:

> *Have at least one person in IT become familiar with physical security strategies, systems, procedures and terminology. Since IT infrastructure has a requirement for physical security, this can strengthen the IT department's position in that regard.*

Until that happens, be gracious in handling your physical security counterparts and keep in mind what it would be like to stand in their shoes: *their security systems are migrating into a technical domain that is foreign to them, yet they must continue to deploy security technology for the sake of the organization's security.*

Physical Security Domain Issues

Just as there are IT domain issues that are unfamiliar to the physical security domain, the reverse is also true. This is because the IT elements of physical security systems are used differently than the same IT elements of business systems. This has both performance design and security implications. While the differences are few, some are critical. Here are two 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).

Fortunately, for security video systems that utilize IT storage systems, as opposed to previous generation digital video recorders (DVRs), the cost of high-capacity storage is a small percentage of the overall video system cost. However, most physical security departments are unaware of this type of storage—Network Attached Storage (NAS) and Storage Area Networks (SAN), for example. They are also unaware of the fact that such storage is much more robust than that provided by DVR solutions.

Thus another good strategy for IT departments is:

> *Obtain use cases for scenarios that involve security system communication over the corporate network, and work with physical security's systems integrator in developing network bandwidth requirements.*
>
> *Request use cases for security normal operations and incident response operations from physical security, as the basis for video bandwidth and storage capacity requirements, including the quality of video required for monitoring and investigations purposes. Use worst-case scenarios for maximum capacity requirements, and expect that the maximum network and system capacities will be seldom used, but when required will be critically needed. Also keep in mind all of the network locations from which video may be accessed for incident response.*

Non-Security Benefits to Your 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.

Thus there is a strategy for IT departments to add more business value for IT services:

> *Be attentive for opportunities to apply physical security technology for business purposes, to increase the value of IT services to the business.*

Roles and Responsibilities

When it comes to putting physical security systems onto your corporate network, there are issues new to both the physical security and IT domains. This means 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 will enable a smooth technology transition.

The physical security personnel involved in security technology projects will benefit from learning about the IT department processes used to deploy networked systems and devices. Importantly, 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:

> *Educate your physical security personnel on the IT processes for deploying networked systems and devices, and then establish a cross-functional team with roles and responsibilities assigned appropriately for each group's 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. From the IT perspective, 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.

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 capture 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 your 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 your 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, as every IT practitioner knows. 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 new 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.

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 IT departments is:

> *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.*

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.*

"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.*

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
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 addressing the risks from putting physical security systems on your corporate network, and helping ensure that the business receives the full potential value of the systems.

Addressing the Risks

The twelve measures below provide effective ways to address the physical security technology convergence risks to your corporate network and the systems connected to it. 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 Cisco 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: Require Computer and Network Security

Physical security systems as well as process control systems including SCADA systems (Supervisory Control and Data Acquisition[1]) to date have been sold and installed by system providers without computer and network security being applied to them. This is a consequence of the historical evolution of the systems. Prior to the proliferation of corporate networks in the late 1990's and especially around Y2K, security systems used proprietary communications protocols on closed networks and thus there was no significant need for computer and network security.

Today, corporate network infrastructures span the entire enterprise and are robust enough to be used to connect critical computers and equipment including those used for security. Internet connections raise the threat level very high for unprotected systems and devices. Just as you

[1] A common process control application that collects data from sensors on the shop floor or in remote locations and sends them to a central computer for management and control. The remainder of this paper will omit SCADA systems and address only physical security systems.

require computer and network security for any systems connected to your corporate network, make the same requirement of the physical security systems for both wired and wireless networking.

Many security industry vendors have not adequately considered security in the design, implementation and support of their products. When you find that is the case, document the deficiency and require its correction, or the substitution of an acceptable alternate product.

Here are some features to discuss with physical security system and product vendors.

Secure Management: Prefer the use of HTTPS protocol over HTTP; SSL over telnet; Simple Network Management Protocol – SNMP version 3.0 over 2.0 over 1.0. Use secured remote terminal services (such as authenticated and encrypted connections using Remote Desktop Protocol – RDP).

System Time: Synchronize all systems to a common clock using Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) according to IT's preference, so that event log time stamps are correlated correctly, access privileges expire correctly, and so on.

System Hardening: Ensure all systems are hardened per the manufacturer's specifications. Find out what anti-virus and computer intrusion prevention software is supported to run on the system and then install it in accordance with appropriate IT standards.

Software Maintenance Releases: Find out what the vendor's normal maintenance release cycle is for operating system and application software. Explore if security vulnerability fixes are published and rolled into the maintenance release cycles. Then correlate updates to IT's change control windows so that regular maintenance of physical security systems follows the same pattern. This may require the use of a staging platform for testing operating system and application software upgrades to check for problems before updating the live systems.

Firewalling: Get a list of all protocols and computer ports used for each feature of the security system including but not limited to live video viewing, recording streams, play-back streams, PTZ controls, system configuration, logging, and event notification. Provide this information to IT so that firewalls can be configured to allow the network traffic for the various physical security systems using the corporate network.

Multi-Level Administration: Find out if the security system applications support administrative controls (often referred to as operator controls in physical security) and if those controls can be integrated with your organization's enterprise-wide authentication and directory services. An example set of administration user classes might include: system administrators, operators, viewers, auditors, and managers. This kind of integration can mean that a security system operator's privileges are revoked immediately upon termination, as opposed to requiring that his or her privileges be manually removed from each security system.

Two: Require All Networked Systems and Devices to Meet IT Standards

Ensure that physical security systems, equipment and networks comply with corporate IT standards, and new establish standards for cases where none apply. For example, sometimes specific network switch and router features are required to support security video. Such equipment must be compatible with your existing network and its current and planned future traffic. Where compatibility or performance questions can't be resolved to your satisfaction by technical specifications and reference sites, require pilot tests. Maintaining the manageability of your corporate network is a vital requirement, and you are completely within your rights to require standards compliance for manageability as well as for security, such as Simple Network Management Protocol (SNMP).

Most IT departments are standardized on SNMP 2.0. Don't accept devices that only support the less secure SNMP 1.0, or require their SNMP support to be disabled (in some cases the physical security departments have already purchased and deployed equipment). Don't compromise. For example, require that the SNMP support is sufficient to allow the device SNMP configuration to be set the way you want it to be set.

Three: Direct or Assist in the Network Design and Planning

There are a number of important points related to network design and planning:

- Get involved in the design process early, especially prior to any purchasing commitments being made.
- To capture accurate network requirements, especially network bandwidth requirements, collaborate closely with physical security. Refer to the section early in this paper titled, *Physical Security Domain Issues*, for examples of the kind security system requirements information that must be obtained.
- Dig deep enough into issues that can impact the network and its usage. For example, for some situations multicast video technology (as opposed to unicast) can significantly lower the network bandwidth requirements.
- Where security systems integrators are designing or providing some or the entire network infrastructure, require written documents (electronic or printed) for network design, and also require complete network equipment lists that include make and model. Verbal information and assurances are not sufficient and reluctance to provide proper documentation should raise your suspicions.
- Often IT can contribute to the project by providing up to date network drawings and design documents. Where you can facilitate the design work for physical security systems by providing that information, do so—always, of course, under appropriate terms of non-disclosure with reliable companies.
- Physical security system planning and design can also be affected by planned network expansion or enhancements. Be sure to include such information in planning and design discussions with physical security project team members.

Four: Collaborate on Technology 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 physical security system requirements.

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.

Beyond providing information on IT's technology lifecycle planning, IT can help the physical security department adopt technology lifecycle planning for the physical security systems to the benefit of both departments. This is another opportunity for you, IT, to provide more value to the business.

Five: Provide Technology Evaluation for the Software and Hardware IT Elements of the Security Systems

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.

Six: Plan or Help Plan the Systems Deployment

Most large physical security department technology projects run significantly over schedule, and for the majority of projects the issue is project planning and execution. For projects that involve the corporate network, consider it mandatory that IT is involved in planning the deployment. For large projects whose duration will be more than six months, especially where multiple physical sites are involved, plan to provide one FTE from IT for 75% of the project time. If an IT budget cannot account for that resource, the physical security department's project budget will have to incorporate it.

Seven: Require the Written Planning and Execution of a Complete Acceptance Test Plan

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*.

Test scenarios (a scenario is a brief description of an event) describe the various ways that the end user wants to use the system for normal operations and also for emergency or incident response. As described earlier in this paper, if a security incident occurs, will there be many people trying to access the system simultaneously via the corporate network or the Internet? If so, the system must support that and testing must demonstrate successful performance for that scenario.

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.

Eight: Ensure That System Design and Deployment Meets Corporate Privacy and Data Security Compliance Requirements

Although compliance with corporate privacy and data security requirements is an important point, IT is used to handling it. Today many security systems exchange data with an HR or IT information system (such as a corporate directory system). In such cases this element comes into play. It is important for IT to document any privacy and data requirements that apply as early in the project as possible, so that compliance can be incorporated into the system design and planned usage early on. IT should be prepared to help with policy and procedure development relating to compliance assurance and audit requirements.

Nine: Provide Systems Maintenance Under an IT Department SLA

Many companies are discovering that their IT departments, who are on-site and usually can respond in an hour or less, can provide better service for the computer-based and networked physical security systems than the system provider who installed them. Many IT departments are entering into Service Level Agreements with their physical security departments to provide first response in case of a security system computer or network problem. They send both physical security and IT personnel for factory training on the security systems, and get them certified on them as appropriate. In most cases this approach can significantly reduce the cost of outside maintenance contracts, in addition to reducing compute and network down-time.

Ten: Implement Authorization, Accountability and Auditability Controls

When physical security systems are implemented as a standalone system for each facility, supervising and auditing the operator activity can be a simple task. For enterprise systems whose scope is regional or enterprise-wide the number of operators and amount of system activity is no longer easily supervised or auditable on a manual basis. Yet, as part of a critical security infrastructure, operator authorization, accountability and auditability are critically

important. Establish such controls as a requirement for physical security systems, and where they are not available implement a third-party solution that provides them.

Eleven: Support Unified Security Initiatives such as Role Based Access Control and the Use of a Single Security Smart Card for both Physical and Logical Security

Role Based Access Control is slowly being adopted by an increasing number of physical security departments, especially for organizations that must comply with the U.S. federal government FIPS-201 standard to deploy a single smart card for both physical access and information system access. Datamonitor reports significant savings for single card initiatives, as much as $2 million in annual savings for a 2,000 employee enterprise. (Download the Datamonitor report from the *Security Management* magazine website: http://www.securitymanagement.com/library/smartcards0605.pdf.)

Twelve: Treat the Physical Security Systems as Other Corporate Critical Data Systems Are Treated

Include the physical security systems in automated backup and offsite data backup schedules as is done for corporate critical data systems. Include the systems in corporate business continuity and disaster recovery planning as well.

Conclusion

There is tremendous value added to the business when IT departments support their physical security departments 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 physical security departments, "Ten Rules for Putting Your Physical Security Systems onto the 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."