CONVERGENCE

The Integration of Physical and IT Security

Ramiro Buenrostro
Lewis University
December 2009

ABSTRACT

The purpose of my project is to provide a roadmap for an organization to couple more closely their cyber and physical security efforts. I will concentrate on the integration of access control and closed circuit television systems with the IT infrastructure. I will be analyzing and reporting on the CISCO Physical Security product line. I will research strategies for integrating physical security with the IT infrastructure. I will document the different components necessary to integrate systems. There are organizational case studies of projects that have been successfully completed that I will discuss.

My goal for this project is educate the reader on this growing trend in Information security, discuss implementation strategies to achieve a more holistic security infrastructure, and introduce the reader to one of the product lines available in the market.

Introduction:

There has been a growing trend recently in the information technology world. Network security departments and physical security departments have begun to integrate their security systems into one system. Until recently, most organizations' physical security systems and cyber security systems have been operated as two separate structures by two separate departments. The IT department controls cyber security, which includes access to the internet, all servers, and database applications. The facilities department or management company controls the physical security of the building which includes employee badging, door access to building, security systems, fire alarm systems, and CCTV.

Increasing physical security threats, reducing costs, increasing efficiencies, emerging technologies, and growing risk management issues are driving forces that are making organizations reevaluate their security policies. Organizations in the past have been reluctant to merge these two separate structures because the technology was not available, costs associated with the convergence were high, and the projects were complex. In the past decade, physical security systems have begun to evolve to understand Internet Protocol (IP). The number of devices like cameras, card readers, smart cards, and access controllers that are now IP-capable is growing by the day. For these reasons many organizations are now considering the convergence of these two separate technologies.

Increasing Security Threats:

Since the terrorist attacks on September 11, 2001, the federal government has been a driving force of converged technologies. These attacks changed the security perception in our county and initiated a greater security focus. The office of Homeland Security is driving the policies and conformance by corporate and civil organizations.

In August 2007, President Bush issued HSPD-12 (Homeland Security Presidential Directive 12), which mandates, a secure and reliable form of identification card for millions of federal employees and contractors.[1] This issued ID badge would control physical and logical access to all federal systems and facilities. In response to HSPD-12, the NIST (National Institute of Standards and Technology), drafted standards that defined how to comply on a technical level. Last year Forrester Research projected a tenfold increase in U.S. spending on merging physical and logical access control, across both the public and private sectors, from $691 million in 2005 to more than $7 billion in 2008. [2]

All corporate assets, from office equipment to employees and their belongings need to be protected. Hackers, industrial saboteurs and terrorists must be prevented from infiltrating networks, applications, databases, and building facilities. Corporations and businesses have the responsibility to protect private customer and employee information, protect building facilities, mitigate cyber threats, and meet government compliance. Greater security focus has produced strong governmental regulations and restrictions that companies have to comply with in regards to reporting performance, releasing financial data and protecting customer/employee data. Converged security solutions enable organizations to comply with data collection and data protection regulations like the Heath Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), and Homeland Security Presidential Directive (HSPD-12).

Costs Benefits:

Converging physical security with IT provides cost savings for organizations. Most organizations today already have an IT infrastructure in place, using this existing network and cabling will eliminate the costs for cable and cable installations costs dedicated to the physical security system. Using equipment that connects to and communicates over the existing IP network infrastructure greatly reduces the expense involved with deploying equipment or establishing entirely new sites. Integrating these technologies also allows for centralized monitoring and management of physical security, which results in less need for on-site personnel and reduces licensing costs for hardware and software.

[1] http://hspd12.usda.gov/about.html
[2] http://www.networkcomputing.com/print_entry.php?eid=61439

Increasing Efficiencies:

Physical security and IT convergence will enable vendor-neutral interoperability among diverse security components to support the organization's risk management needs. As physical and IT security merge, networked computer technology and its associated applications will provide organizations with increased operational efficiencies and intelligent security.

The integration of physical access technologies, such as magnetic or proximity cards and readers, with identity management and user authentication technologies, such as tokens and biometrics, allows an organization to establish and manage a single, consolidated database for all authentication credentials and to have a centralized means of setting access privileges for both physical and logical resources said Gregg LaRoche . Gregg LaRoche is the director of product management for Imprivata, Inc., an enterprise authentication and access management appliance company that helps companies secure their Networks, applications, and integrate building and IT access. In an article he wrote for InfoSec.com, he stated that "By linking the two access security systems, companies can extract more value from the badges and proximity cards that they've already deployed and fully leverage their existing infrastructure of readers and doors controlled by physical access control systems."[3] This is an essential goal to the integration process of physical access technologies with identity management and user authentication technologies.

Gregg LaRoche stated that "by incorporating data now available on user location, time of badge-in and badge status within the organization's network/remote access policy, companies are able to enhance their overall security posture." He also stated that "The integration of building access with network security lets the two types of security solutions compliment and reinforce each other. The synchronization of these two systems leads to stronger, more integrated security, as convergence allows organizations to manage network security under a single umbrella." An example he used is that a person will not be able to login to their network applications unless they first had been granted access to the building via a valid card access read. This prevents unauthorized users from remotely trying to login to the network when that user is currently in the building.

Integrating these technologies will also expedite the removal of user access rights, in case an employee gets terminated, suspended, or resigns from the organization. Convergence will allow all building and network access privileges to be terminated simultaneously. With physical and logical systems fully integrated, real-time response to network alarms and emergencies will be possible because convergence enables consolidated logging of entry and access records by true user identity, companies can easily create a more accurate occupancy roster list, knowing exactly where employees are in the event of emergency.

[3] http://www.infosectoday.com/Articles/convergence.htm#author

A real world example of this efficient implementation was conducted by Microsoft Corporation. They describe the process in a Technical White Paper created by Microsoft called Physical Security at Microsoft, Taking Advantage of Strategic IT Convergence, published in September 2009. [4] In a paragraph titled Provisioning Life Cycle, it states that in a traditional solution for physical access security, the process of creating new accounts, granting and maintaining user rights, and revoking accounts when the access is no longer valid is both manual and separate from other human resources (HR) and IT account-creation processes. These limitations make the process more cumbersome to manage. They also often cause errors regarding data accuracy, delays in the setup of user rights, and removal of user rights after an employee has been removed from the other HR and IT systems.

Converging physical security with information technology helps Microsoft solve these problems. Microsoft ties the process of creating, maintaining, and revoking physical access accounts and user rights into the setup and termination infrastructure. Microsoft developed an efficient system for creating network accounts and issuing physical access cards. The Microsoft system uses existing information, rather than collecting the same data repeatedly, to create the accounts as part of the process that adds the user to the HR system. When a manager hires a new employee, the manager adds the initial information into the systems applications and products (SAP) or enterprise resource planning (ERP) system via HeadTrax. HeadTrax is a Microsoft internal HR system that is built on .NET and that ties together HR and SAP systems. An application called ACCMAN automatically adds user accounts to the Active Directory® infrastructure where network access credentials are managed. This new account information is extracted from a data warehouse that is updated daily. Their OnGuard physical access control system creates new accounts and updates relevant data from the HR system by using the data warehouse. This relation of user rights for physical security to the user's role and status in the HR system improves the efficiency of account creation, maintenance, and revocation.

[4] . *download.microsoft.com/download/5/f/e/.../**PhysicalSecurity**TWP.doc*

Convergence Strategies:

Up until this point I have discussed many topics relating to the convergence of physical and IT security. I've discussed security threats, benefits and efficiencies of convergence. In this next section, I will discuss strategies on how to get there. There are many ways to accomplish this process; I will discuss two different strategies on how to maximize the success of convergence for an organization using the industries' best practices.

Every organization has its own security needs and concerns, as well as its own business goals. One way to begin identifying and prioritizing an organization's key convergence goals is to consider common business drivers and their relationship to security convergence. Risk management is a common security-related business driver. Organizations are all faced with different levels of risk. Risk Management is a business function that involves the identification and acceptance or offsetting of risks that threaten the profitability or productivity of an organization

I will introduce The Open Security Exchange (OSE) Convergence Roadmap, which describes a clear and easy to follow path to converge. The Second strategy I will introduce is the Microsoft Convergence Strategy. Microsoft's strategy for developing the processes and solutions that help provide physical security includes a partnership between the internal Global Security and Microsoft Information Technology (Microsoft IT) teams.

The Open Security Exchange(SM) (OSE) is a not-for-profit association of security experts that provides a forum for end-users, manufacturers, integrators, consultants, and allied organizations, to mutually define opportunities for converging physical and IT security.[5] The Convergence Roadmap provides a framework for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build value.

OSE Convergence Roadmap:

The OSE Convergence Roadmap consists of Business Drivers, Strategic Milestones, Tactical Milestones, and Operational Milestones. The roadmap identifies business drivers and strategic plans to achieving the numerous business goals of security convergence.

1. Business Drivers:
Best practice steps states that organizations should focus on business drivers when developing a convergence plan. The security department's objectives should align with the organizations objectives, if they don't, the convergence initiative will be difficult to achieve. The goal is to help align your security department's operational activities, strategic direction with your business value. Each organization's business drivers are different, so each organization must choose the best drivers for their plan. However, the common business drivers and their relationship to

[5] http://www.theose.org/uploads/Convergence_Roadmap_2008-v1.0.pdf

security convergence will help one get started in identifying and prioritizing key convergence goals.

Common business driver include:

1. Compliance
2. Asset/Personnel Protection
3. Shareholder Value/Business Development
4. Cost Control/Productivity

Compliance:
Organizations are required to comply with certain governmental mandatory actions and outcomes, these actions and outcomes are common to IT and physical security. This driver involves staying aware of changes in the requirements themselves, communicating the requirements to the organization, detecting and correcting any non-compliance, capturing and organizing an effective audit trail, and periodic reporting to the appropriate authorities. Compliance must be achieved at the minimum possible cost without sacrificing compliance or performance.

Asset/Personnel Protection:
The purpose of IT and physical security is to protect the organization's revenue producing assets. These assets are people, equipment, products, tools and information. Organizations need to understand which assets need to be protected and what level of assurance is required, then organizations must develop and operate a mechanism to grant access to those assets.

Shareholder Value/Business Development:
Most organizations treat both physical and IT security as a necessary cost of doing business, not as revenue or profit enhancer. Although there is a benefit to a safe work environment,[6] it difficult to quantify the business building benefits derived from this.

Cost Control/Productivity:
Both IT and physical security require investment to lower risk. Both strive to operate on an "efficient frontier" curve. This curve represents security investment versus risk. The goal is to move the curve by lowering costs for all risk levels. Each point on the curve represents the lowest risk for a given investment and/or the lowest cost for a given level of risk.

[6] http://www.theose.org/uploads/Convergence_Roadmap_2008-v1.0.pdf Section 6.3 Business Development

The Efficient Frontier Curve (Illustrated in Figure 1) each point on the curve representing the lowest risk for a given investment and/or the lowest cost for a given level of risk.

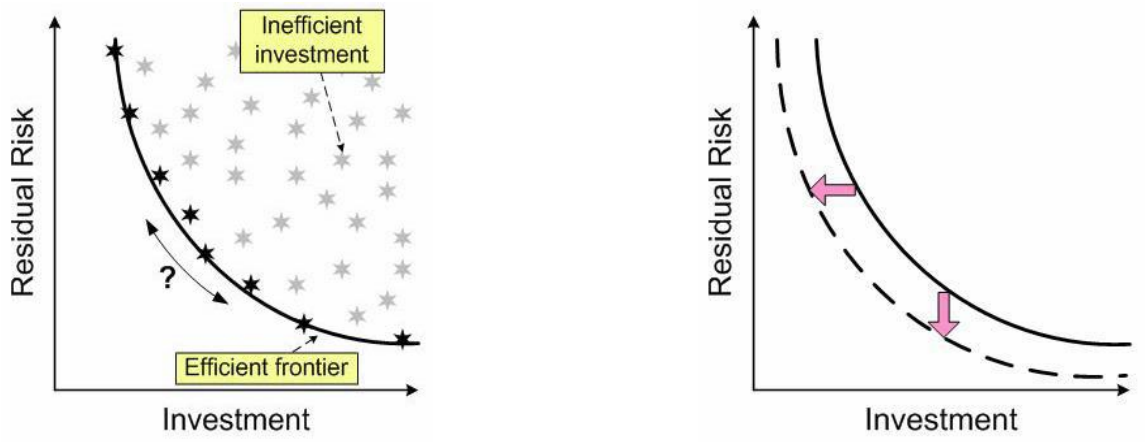


Figure 1, Depicts the Efficient Frontier Curve[7]

2. Strategic Milestones:
The Strategic Milestones are critical to the convergence process because they uniquely define the security organization's character and are fundamental to the success of the security operations. Strategic Milestones include security programs, security governance, process monitoring, regulations, risks, laws, awareness, organizational security, and polices. Only the milestone that will affect the convergence process must be included in the evaluation.

3. Tactical Milestones:
Security executives are responsible for defining big-picture strategies for a Security Organization. However, for the purpose of security, it is necessary to create smaller goals and processes supporting corporate business drivers. Security executives and their teams should focus on delivering tactical targets to provide maximum support for business drivers, and engage business decision-makers when those goals threaten to disrupt business operations. Tactical Milestones include vulnerabilities, metrics, threats, data classifications, security audits, risk analysis, and compliance.

[7] http://www.theose.org/uploads/Convergence_Roadmap_2008-v1.0.pdf.

4. Operational Milestones:
Operational Milestones describe the operations that are normally conducted in the course of achieving corporate business drivers. The operational milestones highlight business processes associated with the Security operations, relationships or dependencies. Examples of Operational activities are access control, training, self assessments, due diligence, enforcement, and IT security.

The OSE Convergence Roadmap will assists organizations identify the proper business reasons for implementing a converged security approach. Cost control, productivity, compliance, asset and personnel protection, and revenue enhancement are clear, measurable reasons that when coupled with unique requirements will help define a clear roadmap for convergence. This roadmap will help identify security gaps caused by different technologies and demonstrate a transition plan to bridge those gaps. The OSE provides a convergence roadmap case study that I will discuss in the following paragraphs.

Baxter Healthcare is a global medical products and services company with expertise in medical devices, pharmaceuticals and biotechnology. Baxter's (375,000) square foot facility is located in Cherry Hill, N.J. Baxter's Cherry Hill Security Department is focused on the principle of how can they add value to their business.

The first process to Baxter's security team Security Master Plan was to interview their primary customers, which in this case is their internal management team. With cooperation of their internal management team, Baxter's security team identified the critical assets in each area of their business. Once the critical assets were identified, they consulted with them about potential threats to those critical assets.

The next step to the process was to determine which security measures i.e. people, process, and technology to employ. Their goal in this process was to align their security operations with the goals and objectives of their business. The security administration team identified four key business drivers that impact their security operations: Compliance, Risk Management, Fiscal Responsibility, and Business Development. I will describe how these business drivers pertain to their situation.

1. Compliance:
This facility manufactures small-volume injectable medications, federal compliance requirements include FDA and DEA regulations that apply to the handling of the pharmaceutical ingredients from initial receipt through manufacturing, to warehousing and shipping. Fire regulations and building codes provide additional compliance requirements.

2. Risk Management:
The team asked what level of risk is acceptable and what level of cost is acceptable?

3. Fiscal Responsibility:
The security team needs to understand the competitive nature of the business and the need for ongoing cost management across the organization. They need to understand the value of applying Lean concepts[8] like 5s, Kaizen, and workflow improvement.

4. Business Development:
The security team realized that a well documented and visibly well-run security program could be used as a tool to differentiate this plant from its competitors.

Security Manager Derrick Wright was the convergence project leader; he mapped Baxter's Healthcare business drivers and aligned the security organization's objectives using the detailed roadmap. The goal of this exercise was to align operational activities, strategic direction and come up with transition plan.

A key strategy of the Security Master Plan was to deploy an enterprise security system that enabled centralized physical identity management for employees, contractors, and visitors. The system also required role-based access management for facility access, self-service administration for security services, and real-time FDA/DEA compliance enforcement for access to regulate areas of the facility. To provide these functions they used Quantum Secure SAFE software.[9] SAFE provides rules-based monitoring and enforcement of compliance requirements, and integration between security processes (such as facility access management) and business processes (such as on-boarding and off-boarding of employees and contractors).

I believe that the OSE's Convergence Road map worked well here because it was a well planned process. They started by identifying their critical assets and the potential threats to those assets, this is a very important step in this process, identifying what to protect. In their next step, they identified security measures and the business drives that would impact their operations. This step eliminates organizations form wasting time and resources on business drivers that don't impact their operations. Once the planning was done, deployment of the security system that would integrate these processes would take place.

[8] http://en.wikipedia.org/wiki/Category:Lean_concepts
[9] http://www.quantumsecure.com/Products/SAFE-Physical.aspx

Microsoft's Convergence Strategy:

Microsoft's convergence strategy is based on a design philosophy that includes a strategy for managing physical access to their resources and the Weighted Business Model. The Weighted Business Model (illustrated in Figure 2) incorporates the balance between technology, monitoring, and response, and the administration of all three.

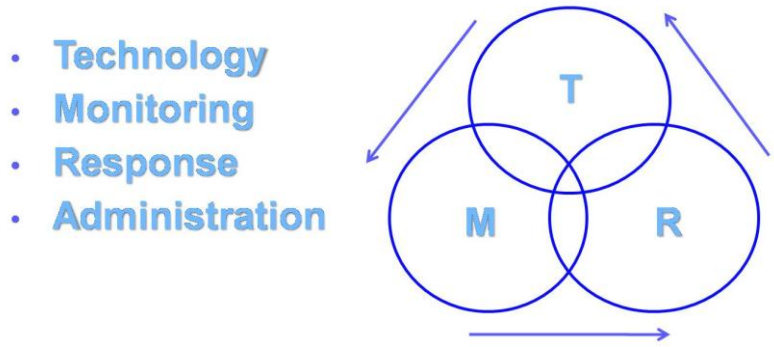


Figure 2, Depiction of the components of the Weighted Business Model

The strategy used at Microsoft for developing the processes and solutions that helped provide physical security included a partnership between the internal Global Security and Microsoft Information Technology (Microsoft IT) teams. The Weighted Business Model assisted Global Security understand and define the key components of physical security and their relationship with each other. This understanding enabled the team to implement an effective and efficient strategy.

The next key component of the convergence process was the cooperation of the different departments and teams within Microsoft. . A fundamental part of this cooperation was establishing relationships and expectations between the various entities. Global Security then developed security objectives to meet the unique needs of the business across all regions by analyzing the functions of the organization, and by understanding the benefits and pitfalls of different approaches. To produce the physical security design, Microsoft managers agreed to a basic set of design principles and continually used them as the touchstone for new decisions. This enabled them to maintain the integrity of their design. The following design principles represented the business parameters and functional design elements that Global Security focused on.

[10] *download.microsoft.com/download/5/f/e/.../**PhysicalSecurity**TWP.doc*

1. Deterrence Value:
Security measures must strike a balance between security and functionality. The strength of this balance is creating awareness of the existence of physical security; security measures should be conspicuous and strategically placed.

2. Remote Monitoring:
Monitoring security systems from a remote location provides the ability to centralize the administration and response of physical security systems. Remote monitoring also allows remote functionality to maintain and troubleshoot the physical security equipment over the network.

3. Precision Response:
This solution must provide for precision response, it also must ensure that the proper resources can be dispatched on site in a timely manner when an event is detected. Microsoft can remotely assess incidents and dispatch an appropriate response.

4. Off-the –Shelf Infrastructure:
Microsoft used standard off-the-shelf hardware and software, this allowed the Global Security team make a conscious decision to adapt its processes to the infrastructure and not the other way around. The use of off-the-shelf products reduced the costs of both implementation and maintenance, while increasing continuity and efficiency in delivery because Microsoft can apply standard training and support services.

5. Use of Microsoft and Partner Products:
Global Security analyzed various Microsoft tools and applications and used them to deliver much of the core technology of the solution, Microsoft products where used when possible.

6. Remotely Managed IP Devices:
Microsoft used the existing global IP network to handle rapid changes in hardware and to achieve faster and more cost-effective scalability. Using their network allows Microsoft install security devices, like IP cameras and card readers, more efficiently because installation is less likely to require additional proprietary components or a separate cabling.

7. Defense in Depth:
Defense in depth is a very popular strategy in the industry; I will list some of the key resources on the strategy pertaining to Microsoft. Defense in depth provides multiple layers of security at facilities that are appropriate to assert risk. The foundation of this concept is that requiring additional security controls, or layers, along with an approach to protect critical assets, develops a mechanism to systematically delay, effectively intervene in, and mitigate risks. A threat that infiltrates one layer is detected at another layer, giving Microsoft multiple opportunities to detect and respond to an event. Defense in Depth for physical security begins with incorporating physical security into the design of facilities. The design considers all property boundaries, buildings, parking areas, and flow of human traffic through the building. The design also

considers physical security devices. All of these functions combined provide a layered defense strategy in protection of Microsoft resources. [11]

8. Forensics/Investigative Model:
A critical component of the design philosophy is to ensure that video data, access logs, and other pertinent information are properly captured and stored for investigation if a physical security incident occurs. If an incident does occur, the security team must be able to retrieve and analyze stored data and log information.

9. Reliability:
An infrastructure must be reliable, and it must work when needed. Access control can be used a metric to determine reliability. How often does an access card get scanned at a reader and it does not open a door, or when a user logs in to the network will the system allow access. If the system is not reliable for access control productivity will be impacted. Compliance may also be a metric to measure reliability. If an organization is not compliant to its corporate and or governmental policies, it may not be able to conduct business in a timely manner. The organization may also be levied fines for non compliance.

10. Sustainability
Sustainability is the ease in which a new infrastructure or device can be maintained and supported. As the environment continues to grow and systems become more complex, sustainability will be crucial to keep support costs low.

These design principles helped Microsoft and the Global Security team on how use the IT organization, Microsoft technology and products, and third-party resources to provide physical security services to Microsoft personnel and locations worldwide. The principles and techniques that were discussed in Microsoft's Technical White Paper may be employed to manage physical security in any organization.

Emerging Technologies:

In the last section of this paper the focus has been on some of the strategies available for the convergence process of physical and IT security. In the next section I will focus on emerging technologies available to implement theses strategies. In the last ten years, Internet Protocol (IP) has become the de facto standard for physical access system devices which means physical security and IT have begun to speak with the same language. Because of this, the list of access devices that are now IP-capable has expanded considerably including smart cards, cameras, card readers, and access controllers. [12] These new technologies have made the integration of physical and IT security possible. In the following paragraphs I will discuss some of these new technologies.

---

[11] download.microsoft.com/download/5/f/e/.../PhysicalSecurityTWP.doc Defense in Depth page 7

[12] http://www.articlesbase.com/print/1234839

CONVERGENCE

Smart Cards:

Smart cards are tokens that bridge the gap between logical and physical security. The card has the capability to hold a picture ID and other printed identifiers, including the cardholder's nature, fingerprint or other biometric identifiers. Smart cards can provide several security-level options ranging from simple access control to complex data encryption. The card is embedded with two chips. The first is a programmable chip that is used with a card reader to authenticate the cardholder to computers and data. The second chip is the proximity chip, which is used for access to facilities and building. The existing space for the electrically erasable programmable, read-only memory (EEPROM) smart cards is 8, 16, 32 and 64K (kilobytes). Smart cards provide confidentiality, authentication, and non-repudiation for practical IT uses by using a unique serial number and a Personal Identification Number (PIN) to identify a user, prove identity and grant network access. By combining smart cards with Public Key Infrastructure (PKI), the cards can store the algorithms, keys, and certificates required to encrypt confidential information.

Smart cards are available for physical access control in either contact or contactless formats. In contact card format, smart cards use an eight-pin contact, micromodule to physically connect to the card reader. The contact format is older technology that is being replaced by the newer contactless format because of card reliability issues. The contactless smart card format uses an antenna with approximately a 10-centimeter (cm) range to communicate with the reader. These cards derive their power from a radio frequency (RF) generated by the electromagnetic field produced by the card reader antenna. The RF field also transfers information to and from the card and card reader. The fundamental benefit of using a smart card for both physical and IT security is enhanced security due to the use of multiple factors in authentication; both a card and a PIN are required to gain access. Smart cards can improve return on investment, through the elimination of multiple passwords and increased transparency that eliminates abuses, such as credential sharing.

In November of 1999, the Deputy Secretary of Defense directed the Military Services to implement smart cards in the form of a Common Access Card (CAC).[13] The CAC has numerous functions; it enables physical access to buildings and controlled areas, access to computer network and systems as well as serving as the primary platform for the Public Key Infrastructure (PKI) token. Today, the Department of Defense CAC program is the largest deployment of cryptographic Smart Cards for information security.

IP Cameras:

Using IP-based video greatly reduces the cost of a video security system, while simplifying deployment and monitoring of video cameras. The average data rate for a video surveillance camera is between 2 and 4 Mb per second, so a 100 Mb network switch running over fiber can handle up to 25 cameras. The same fiber cabling can support 1 Gb switches, which makes it possible to support many more cameras on a single cable.

[13] http://www.cac.mil/assets/pdfs/DEPSECDEF_Policy.pdf

Network IP cameras connect to a computer network. They each have respective nodes, or network addresses, and act as video servers on the network. This allows a user to view the video from any computer equipped with a web browser such as Internet Explorer. IP cameras use the same cat5e cable used for networks, so no special cables are required. With this single cable the camera can be powered and communicate to the network. These new IP cameras can also be power through Power over Ethernet (PoE), so a separate power source is not needed. Network cameras can plug in to any computer jack available on the local network. Surveillance can be handled remotely from anywhere in the world, as long as a user knows the IP address of the camera. Numerous protocols are used depending on the make and model of the camera, including TCP/IP, HTTP, and FTP.

When dealing with video streaming a major concern is bandwidth consumption. Each camera requires its own data stream. Newer video data compression techniques have helped, but it's still an issue because quality video streams can take up to 4Mbps of bandwidth per camera. A solution to this bandwidth problem is called Video Analytics.[14] Some IP cameras include video analytics software embedded on chips in the camera. Video analytics systems can identify an alarm on specific behaviors programmed into the camera. By analyzing individual pixels in a frame, analytics can distinguish between a vehicle and a person. Video Analytics allow you to input what actions you want to be notified about, the camera then will only sends those clips. This saves bandwidth and recording storage space.

In the next section of this paper I will discuss the Cisco product line that allows the integration of physical and IT security. I will describe in detail the components necessary to complete an integration project.

CISCO PYSICAL SECURITY SOLUTIONS:

Cisco's physical security solutions provide broad network-centric capabilities in video surveillance, IP cameras, electronic access control, and groundbreaking technology that converges voice, data, and physical security in one modular appliance. Cisco's Physical Security software and hardware facilitates the capture, transmission, viewing, recording, archiving, and management of analog and IP video sources and provides electronic access control.
In April 2008, Cisco announced key additions to its Cisco Connected Physical Security product portfolio. These new key additions are the new high-definition and standard –definition cameras and Cisco's IP-based physical access control system. These new products ease the convergence

[14] http://web.kennesaw.edu/news/stories/converging-security-technologies

of information technology (IT) and physical security by allowing customers to integrate with existing physical security systems and IT infrastructures. [15]

These latest physical security products support Cisco's vision of offering a single unified security product suite that enables users to integrate all security operations within the IP network. Utilizing the network as a scalable platform for integrating security provides businesses with several benefits such as operational flexibility, greater protection capabilities, lower cost of ownership, and reduced risk. Cisco's physical security solutions enables customer to use their IP network as an open platform to build more collaborative and integrated physical security systems while preserving their existing investments in analog-based technology. Bill Stuntz, general manager of Cisco's Physical Security Business Unit stated that "Physical security is becoming tightly woven into the fabric of the IP network, making the industry as a whole extremely exciting." He continued "The network is the platform for connecting physical security systems of all types with other enterprise systems. This development helps bring the promise of converged security to life. Cisco can make this happen because we have the expertise in both IT and physical security to lead this charge. The security industry is very important to Cisco."[16]

Cisco's IP-based Physical Access Control (PAC) system

The Physical Access Control System utilizes the IP network as a platform for integrated security operations. This product includes both hardware and software components and offers a complete solution for IP-based Electronic Access Control. This new access control system is built to work with existing door readers, locks and biometric devices. It targets campus environments and office buildings. The components of the PAC system include the Access Gateway, Physical Access Manager (PAM), and three additional modules; reader, input, and output.

Cisco Physical Access Gateway

The Cisco Physical Access Gateway is the primary means for the Cisco Physical Access Control solution to connect door hardware, such as locks and readers, to the IP network. One gateway can control up to two doors. The access control system can be deployed incrementally or door by door. There is no central panel; this simplifies system design, wiring, and planning, resulting in significant cost savings over legacy architectures. Additional modules can be connected to the gateway, allowing for extensibility. All communication from and to the gateways is 128-bit Advanced Encryption Standard (AES) encrypted. . In wired deployments, the device is capable of being powered by Power over Ethernet (PoE). It's also possible to connect to the gateway over Wi-Fi 802.11a/b/g wireless link. (Figure 3 on the next page illustrates Cisco's Access Gateway.)

[15] http://newsroom.cisco.com/dlls/2008/prod_040208.html
[16] http://newsroom.cisco.com/dlls/2008/prod_040208.html

[17]

Figure 3, Cisco Access Gateway

The Cisco Physical Access Control solution offers the following additional modules that can be connected via a three wire controller area network (CAN) bus.

Reader module: This module can connect to a complete set of door hardware, allowing an additional door to be controlled by the same physical access gateway.

Input module: The input Module can connect up to 10 inputs, each of which can be configured as supervised or unsupervised. The module must be used in conjunction with a Cisco Physical Access Gateway, and cannot be used standalone.

Output module: The Cisco Physical Access Output Module can connect up to eight Form C relay outputs, with contacts rated 5A @ 30V DC or 125VAC (resistive). Each can be configured as either Normally Closed (NC) or Normally Open (NO).

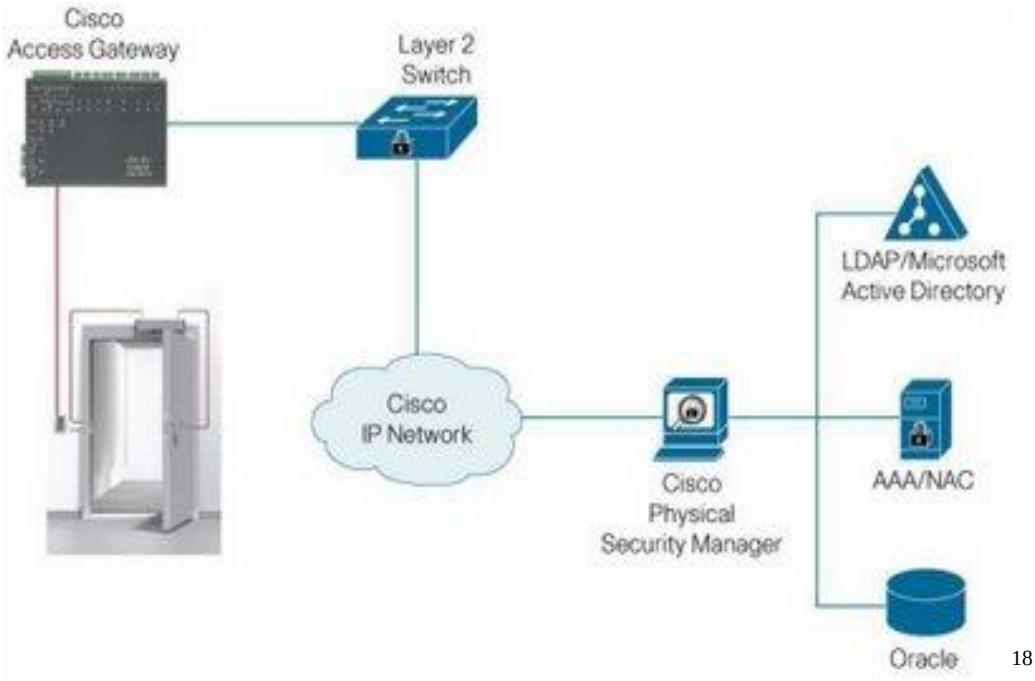
Cisco's Physical Access Manager

Cisco's Physical Access Manager (Cisco PAM) is used to configure gateways and modules, monitor activity, enroll users, and integrate with IT applications and data stores. This application comes installed on Cisco's access control hardware. Cisco Physical Access Manager supports a thin client model. Clients from computers running the Windows operating system can contact Cisco Physical Access Manager and download and install an application that allows interaction with the Cisco Physical Access Manager for administrative purposes.

[17] http://ciscosurveillance.blogspot.com/

Administrative users of Cisco Physical Access Manager can be configured to use Microsoft Active Directory for authentication. You can create access control policies for any person, two-door, anti-passback, etc. PAM also integrates with, Lightweight Directory Access Protocol (LDAP), and some HR Databases. PAM is integrated with the Cisco Video Surveillance family of products, enabling an organization to associate cameras with doors, and to view video associated with access control events and alarms. Cisco Physical Access Manager dynamically acquires camera inventory from Cisco Video Surveillance Manager, associates cameras to doors, and users can view recorded or live video for every event from the door.

Figure 4 illustrates a typical access control implementation using the physical access gateway. The access gateway module controls the door strike or magnetic locks. It then connects to a layer 2 switch that connects it to the internet. From the internet the signal travels to a work station that holds the Physical Security Manager software, which then is managed through their network security infrastructure.



[18]

Figure 4, Typical CISCO Physical Access Control (PAC) Architecture

[18] http://ciscosurveillance.blogspot.com/

Cisco Video Surveillance Systems:

Cisco's video surveillance system has two different formats, the Hybrid Analog and Network-Centric Video Surveillance Products and the Network-Centric Video Surveillance Products.

Cisco's hybrid analog and network-centric products

Cisco's hybrid analog and network-centric products offer network-centric video surveillance software and hardware that supports video transmission, monitoring, recording, and management. These products protect customers' existing investments in analog equipment while enabling these devices to operate as part of an IP network-centric deployment. Cisco products enable any-to-any multivendor device interoperability; this allows customers to build best-in-class video surveillance systems that optimize price, performance, and function. Cisco video surveillance works in unison with the advanced features and functions of the IP network infrastructure, i.e. switches, routers and other network security devices. The components associated with this format include IP Gateways, Convergence Chassis, Service Platform, Integrated Service Platform, and Stream Manager Software.

Cisco Video Surveillance IP Gateways (encoders/decoders):

Cisco Video Surveillance IP Gateway encoders enable a wide range of analog video cameras, including pan-tilt-zoom (PTZ) models, to be connected and controlled over an IP/Ethernet network. Similarly, Cisco Video Surveillance IP Gateway decoders allow users to use their existing investment in analog monitoring displays and keyboard/joystick controllers. The encoders and decoders run Cisco Video Surveillance Stream Manager Gateway software. Cisco Video Surveillance IP Gateway video encoders and decoders use a high-quality H.264 and MPEG-4 video compression technology that allows video streams to be switched over the IP network at up to full D1 resolution, and up to 30 frames per second, while consuming low bandwidth.

Cisco Video Surveillance Convergence Chassis

The Cisco Video Surveillance Convergence Chassis consolidates many physical security functions in to a single, highly flexible and manageable rack-mountable platform supporting a wide range of modular capabilities ranging from video and audio encoding and decoding to alarm contact closure aggregation, and IP / Ethernet network switching. It features a robust 3-RU rack-mountable chassis design capable of supporting extended temperature ranges. With several possible mounting bracket configurations it retains an easily accessible ground lug and rear-panel power switch for quick maintenance and deployment. It has a total of 16 modular slots. The Cisco Video Surveillance Convergence Chassis supports an entire range of Cisco IP Gateway modules, with up to 64 encoder ports in a single chassis. The convergence chassis' backplane, which interconnects all Cisco Video Surveillance IP Gateway plug-in modules and the power supply, is field-replaceable and upgradable.

The Cisco Video Surveillance Convergence Chassis with Fast Ethernet ports

The Cisco Video Surveillance Convergence Chassis with Fast Ethernet ports is the entry-level convergence chassis for direct network connected deployments. It has fourteen integrated 100 Mbps (Fast Ethernet) switch ports. This chassis can support a large number of video streams. It features back-side RJ-45 ports. The chassis allows connected Cisco Video Surveillance IP Gateways plug-in modules to be inserted or removed from the chassis without the need to disconnect the network cable.

The Cisco Video Surveillance Convergence Chassis with four integrated USB 2.0 hub ports provides a quick and easy way to connect to Cisco's video surveillance recording platforms. Up to sixteen 4-channel MPEG-4 Cisco Video Surveillance IP Gateway encoder modules can be placed in the chassis, providing 64 video inputs.

Cisco Video Surveillance Services Platform

The Cisco Video Surveillance Services Platform accepts digitally encoded video from Cisco Video Surveillance IP Gateways or from the Cisco Video Surveillance Convergence Chassis. It’s preloaded with Cisco Video Surveillance Stream Manager software; the Cisco Video Surveillance Services Platform handles video archival and retrieval functions, authentication watermarking, and video data export. For each video stream, resolutions up to full D1 and frame rates up to 30 fps National Television System Committee (NTSC) or 25 fps Phase Alternating Line (PAL) are achievable.

The Cisco Video Surveillance Services Platforms which are displayed on page 22 are available with a choice of a 1-rack-unit (RU) and 2-RU high form-factor. All Cisco Video Surveillance platforms have a Linux Operating System. The 2RU Services Platform features RAID 5 fault-tolerant storage for mission-critical, high-reliability video surveillance operations. Additionally, it features 12 hot-swappable, front-load hard disk drive bays, currently capable of supporting up to 4.8 TB (4.4 TB usable) when using 400-GB SATA hard disk drives. When a new hard disk drive is installed or replaced in the Services Platform, it automatically configures the OS and Cisco Video Surveillance Stream Manager software. For an entry-level recording and storage application, the Cisco Video Surveillance Services Platform 1-RU model provides an economical and compact, easy-to-install, rack-mountable storage solution. Using a JBOD configuration of hard disk drives, this Cisco Video Surveillance Services Platform currently supports up to 1.6 TB of video storage using 400-GB HDD technology.

Figures 5 and 6 display the two different Video Surveillance Platforms, the 2-RU Raid 5 small has bigger video storage capabilities.

Figure 5, Cisco Video Surveillance Services Platform; 2-RU RAID 5 Model, 6x400-GB Hard Drives, with Stream Manager Software

[19]

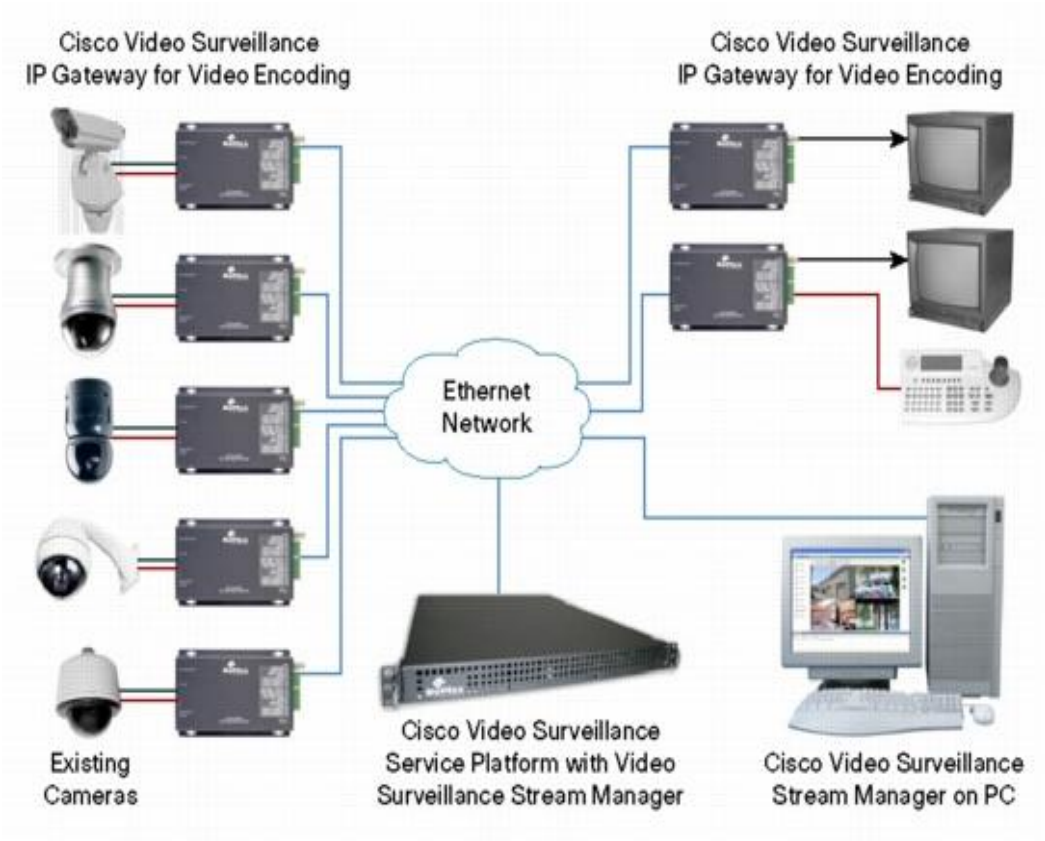
Figure 6, Cisco Video Surveillance Services Platform; 1-RU JBOD Model, 2x400-GB Hard Drives, with Stream Manager Software

---

19

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps6921/ps6938/product_data_sheet0900aecd804a2dbc.html

Figure 7 displays how analog components like cameras, monitors, and matrix controllers integrate with the video server and how they are connected through the network.



[20]

Figure 7, Typical Cisco Video Surveillance Services Platform

[20] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps6921/ps6938/product_data_sheet0900aecd804a2dbc.html

Cisco's Video Surveillance Integrated Service Platform

Cisco's Video Surveillance Integrated Services Platform displayed in figure 8, delivers a cost effective high-resolution digital video surveillance recording solution, replacing analog VCRs. It's designed to work in concert with traditional matrix switch equipment. Cisco Integrated Services Platforms record, and playback video from analog video cameras that are under the control of traditional CCTV keyboards as well as Cisco Stream Manager PC clients. This Platform features a compact, rack-mountable chassis that accepts both NTSC and PAL video inputs from traditional matrix switches for video surveillance recording applications. It's available with up to three 4-channel encoder modules, providing a total of 12 video inputs in a single chassis. It's also equipped with the powerful Cisco Video Surveillance Stream Manager Services software running on a Linux Operating System. The Cisco Video Surveillance Integrated Services Platform handles video archival and retrieval functions, authentication watermarking, and video data export. This platform also features 12 hot-swappable, front-load hard disk drive bays, currently capable of supporting up to 4.8 TB (4.4 TB usable) when using 400-GB SATA hard disk drives. Integrated Services Platforms support RAID 5 fault-tolerant storage for mission-critical, high-reliability video surveillance operations. When a new hard disk drive is installed or replaced in the Integrated Services Platform, it automatically configures the OS and Cisco Video Surveillance Stream Manager software for rapid maintenance or storage expansion.

[21]

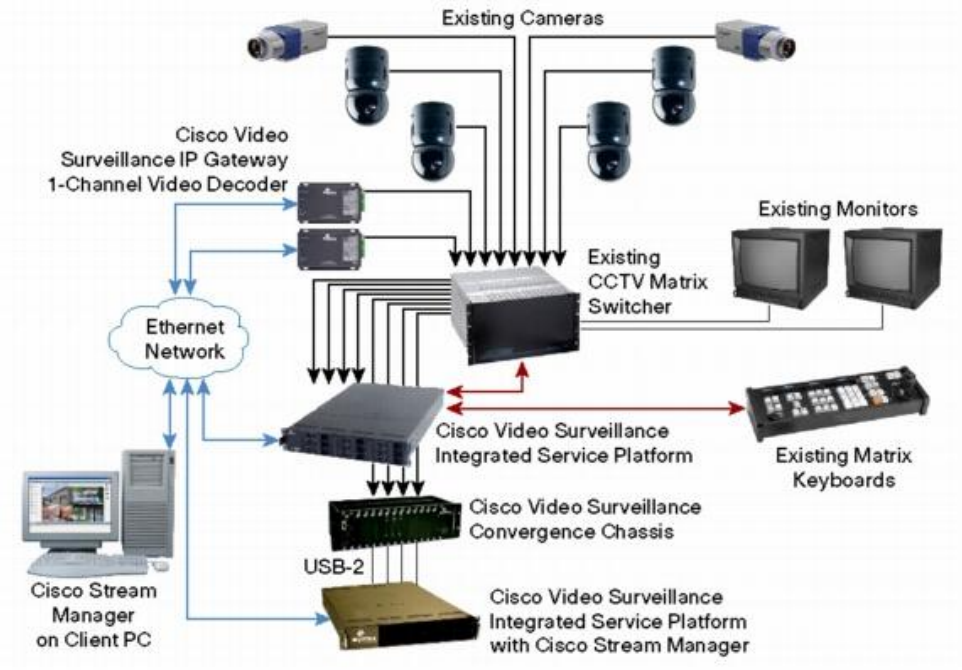
Figure 8, Cisco's Video Surveillance Integrated Services Platform

[21] http://www.cisco.com/en/US/products/ps6939/prod_view_selector.html

Cisco Video Surveillance Stream Manager Software

The software is a collection of discrete software modules that provides advanced and flexible video surveillance system configuration, management, operation, and viewing of live and recorded event-tagged video. The software modules combine the capabilities of many standalone hardware and software systems into one product, including features provided by digital video recorders, matrix switching systems, video multiplexers, and transmission systems. The Cisco Video Surveillance Configuration Module is used for all hardware device programming. It discovers devices automatically, and enables configuration of numerous parameters i.e. device settings-device name, video output, Network settings-IP address, subnet mask, default gateway, Dynamic Host Control Protocol (DHCP), Domain Name System (DNS), Simple Network Management Protocol version 2 (SNMPv2), and quality of service (QoS) in the form of differentiated services code point (DSCP) marking, and many more configuration options.

Figure 9 depicts how the Video Surveillance Integrated Service platform is configured with its various components.



[22]

Figure 9, Typical Cisco Video Surveillance System Architecture

[22] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps6921/ps6939/product_data_sheet0900aecd804aa296.html

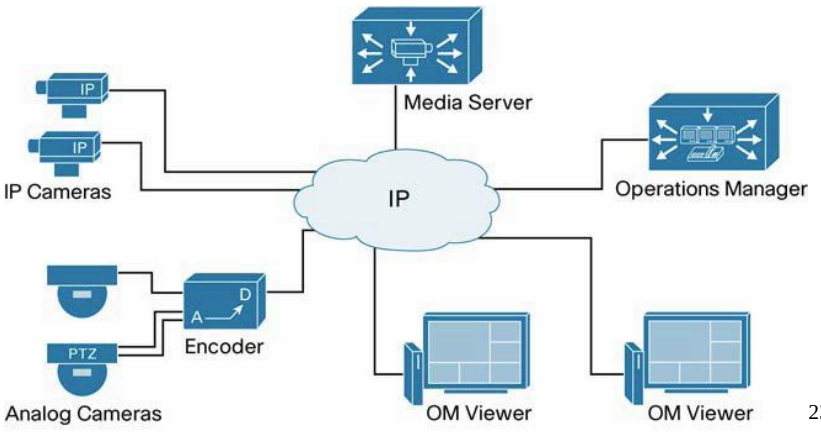
Network-Centric Video Surveillance Products

Network-Centric Video Surveillance Products offers a solution for multiple-site and remote-site network-centric video surveillance. It provides excellent scalability, reliability, and bandwidth management. The components of this format include Media Server, Encoding Server, Virtual Matrix, Operations Manager, Storage System, and IP Cameras.

Cisco Video Surveillance Media Server

The Cisco Video Surveillance Media Server (MS) is the core component in the VSM, enabling distribution, archiving, and management of video feeds. It offers the power and flexibility to meet a diverse range of video surveillance requirements and can coexist on an IP network with other IT applications. Cisco video surveillance solutions work with the advanced features and functions of the IP network infrastructure-switches, routers, and other network security devices-to enable secure, policy-based access to live or recorded video. Cisco Video Surveillance Media Server is fully compatible with other Cisco Video Surveillance Manager applications that provide video display control and distribution (virtual matrix switching), customizable Web-based user interface for roles-based operation and management, system configuration, and options to support storage area networks (SANs) and network- and direct-attached storage (NAS and DAS). Media Server also runs on Linux-based OS.

In Figure 10, the Media Server is responsible for receiving video streams from different IP cameras and encoders and replicating them as necessary to different viewers.



[23]

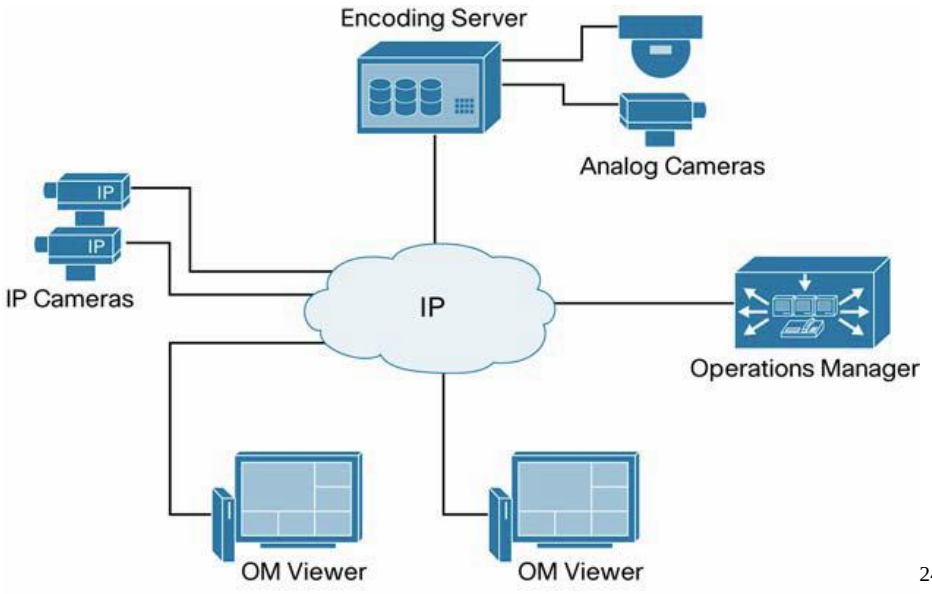
Figure 10, Video Surveillance Media Server

[23] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9145/ps9152/design_guide_c07-462879.pdf

Cisco Video Surveillance Encoding Server

The Cisco Video Surveillance Encoding Server (ES) displayed in figure 8 on page 26 is an all-in-one appliance that encodes, distributes, manages, and archives digital video feeds. Each server encodes up to 64 channels and provides up to 9 TB of storage. It offers the power and flexibility to meet a diverse range of video surveillance requirements and is cost-effective and simple to install. The encoder server combines multiple video codecs in a single encoding. It also manages bandwidth over each part of the IT network to complement capacity and protect other applications. You can also create redundant archives of events or loops and automatically store them in a secure location. With the addition of the Cisco Video Surveillance Operations Manager, the Encoding Server also provides administrators and operators with multiple Web-based consoles to configure, manage, display, and control video.

Figure 11, shows an Encoding Server receiving video streams directly from IP and analog cameras. The analog video streams are encoded into a video stream that can be archived and distributed to the different viewers. The Encoding Server acts as the Media Server and Encoding Server simultaneously.



[24]

Figure 11, Cisco Video Surveillance Encoding Server

[24] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9145/ps9152/design_guide_c07-462879.pdf

Cisco Video Surveillance Virtual Matrix

The Cisco Video Surveillance Virtual Matrix software is a complementary component of the Cisco Video Surveillance Media Server. It enables an intelligent digital video management system that allows any operator or integrated application to control what video is displayed on any number of physical and virtual monitors, both local and remote. It uses the IP network to provide aggregation and transmission of video from cameras and recording platforms much like the function of a classic analog video matrix switch. The Virtual Matrix is easily integrated with other systems to automatically display video in response to well defined triggers. These triggers can include access control and fire systems in buildings, outdoor motion sensors, or even radar systems for military applications. It brings complete flexibility to the delivery of live and recorded video to demanding command centers providing high-availability access to network video for 24x7 monitoring applications.

Figure 12 demonstrates how operators can choose from any number of available cameras to be displayed on any system monitors within any custom video display patterns.

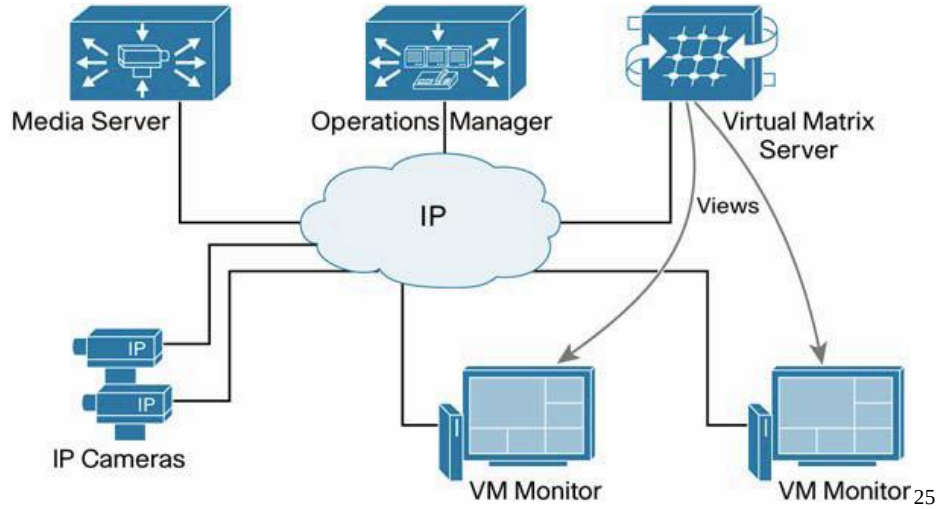


Figure 12, Virtual Matrix Server[25]

[25] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9145/ps9152/design_guide_c07-462879.pdf

Cisco Video Surveillance Operations Manager

The Cisco Video Surveillance Operations Manager is a component of the Cisco Video Surveillance Manager suite of products. It enables organizations to quickly configure and effectively manage complex video applications throughout the enterprise. It meets the diverse needs of administrators and operators by providing multiple Web-based consoles to configure, manage, display, and control video throughout a customer's IP network. A single Operations Manager can manage a large number of Media Servers, Virtual Matrixes, cameras, and users. Viewers can access the Operations Manager via their Web browser. The Operations Manager is responsible for delivering a list of resource definitions, such as camera feeds, video archives and predefined views to the viewer. Once this information is provided to the viewer, the viewer communicates with the appropriate Media Server to request and receive video streams.

Cisco Video Surveillance Storage System

The Cisco Video Surveillance Storage System (SS) provides flexible options for storing video and audio using cost-effective, IT-caliber storage devices. The Storage System allows the Cisco Video Surveillance Media Server’s internal storage to be combined with direct attached storage (DAS) and storage area networks (SANs). Video can be stored in loops, one-time archives, or event clips triggered by external systems. The storage system provides redundant storage and remote long-term archives. The storage system can be expanded as your system or requirements grow. Cisco Video Surveillance Storage System benefits include SAN, NAS, and DAS configurations, internal storage up to 24 TB (on the Media Server), SAN arrays that support up to 42 TB per array, 42TB, Redundant archives, RAID 0/1/5 configuration, Optional clustering for failover protection, online access to video at more than 100 times faster, and Redundant power supplies and RAID controllers.

Cisco Video Surveillance IP Cameras

Cisco's new high-definition and standard-definition IP cameras provide high-quality digital video surveillance capabilities for use in a variety of environments.

The new camera models include the following:

Cisco Video Surveillance 4000 IP Camera is a high-definition camera that combines the best resolution, video compression and intelligent digital signal processor (DSP) available in a single camera. The camera utilizes H.264 Main Profile video compression and a high-speed imager that captures video up to 1920 x 1080 at 30 frames a second. The Cisco Video Surveillance IP camera has an optional high-speed DSP completely dedicated to intelligent video functions such as video analytics. The camera supports Power over Ethernet (PoE) 802.3af, 12 VDC or 24 VAC power through an optional external power supply. The camera provides hardware-based Advanced Encryption Standard (AES). For enhanced bandwidth management, the camera supports IP Multicast. Using IP multicast to transmit video traffic reduces the overall network load and minimizes the impact on the source of the video from unnecessary replication of a common data stream. In IP Multicast transmissions, a host sends one copy of each packet to a special address that can be used by several hosts interested in receiving the packets.

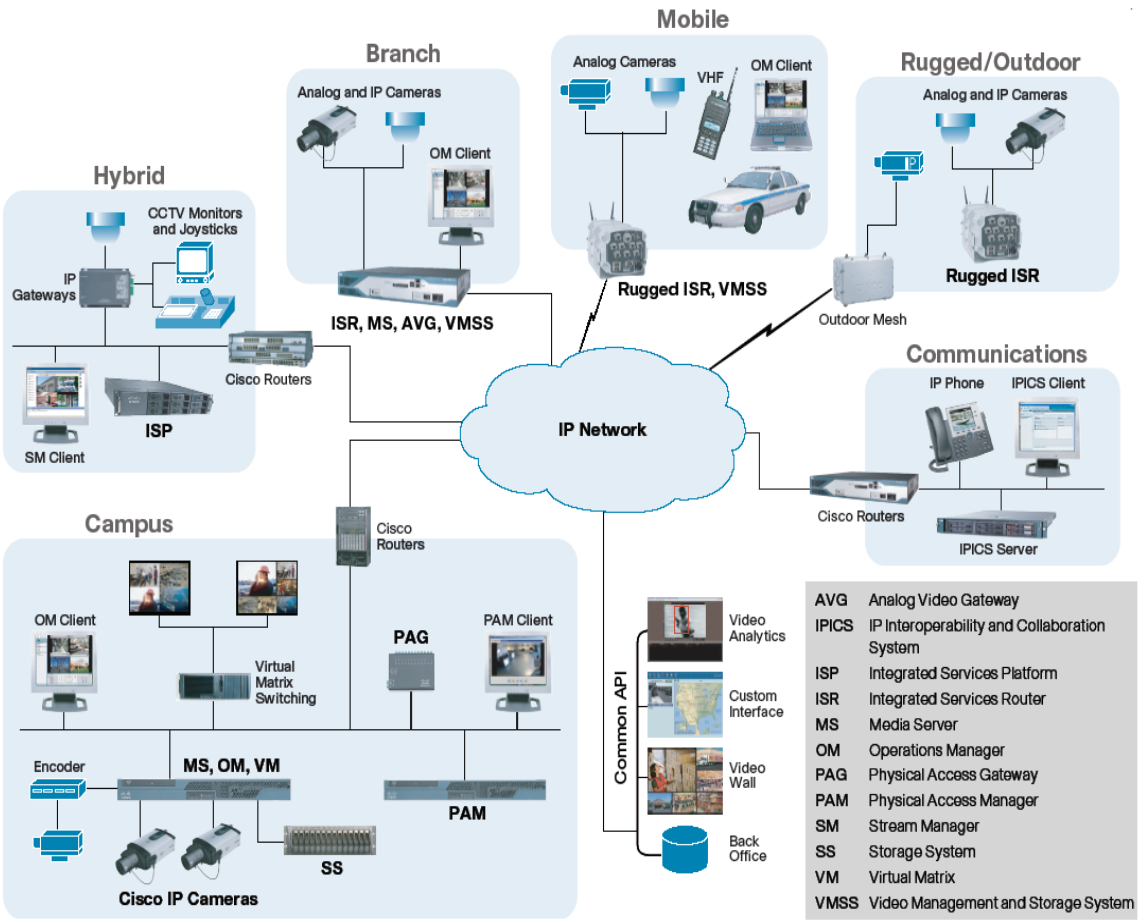
Cisco Video Surveillance 2500 IP Camera is a standard definition camera available either as a wired Power-over-Ethernet (POE) or DC power through an optional external power supply, or as a wireless version supporting 802.11b/g/. The wireless IP camera model is compatible with networks that conform to the IEEE802.11b or IEEE802.11g specifications. The IP camera provides networking and security capabilities, including multicast support, hardware-based Advanced Encryption Standard (AES), hardware-based Data Encryption Standard/Triple Data Encryption Standard (DES/3DES) encryption, and, for the wireless model, 802.1X authentication. Figure 13 illustrates Cisco’s wired and wireless IP cameras.

26

Figure 13, Cisco Video Surveillance IP Cameras (wired and wireless)

[26] http://ciscosurveillance.blogspot.com/

Figure 14 displays Cisco physical security solutions which can be deployed in a wide range of scenarios. These solutions are designed for effective deployment in campus, branch, mobile, and outdoor situations. The video deployments range from a few to thousands of cameras. They can be deployed in LAN/WAN and wireless connections. They will work in indoor and harsh outdoor or mobile environments. Here is an example of a deployment scheme.



[27]

Figure 14, CISCO PHYSICAL SECURITY SOLUTION DEPLOYMENTS

[27] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9145/ps9152/at_a_glance_c45-468316.pdf

The previous page illustrated physical solution deployments; I will know discuss a case study conducted by Cisco's physical security department of real world applications.

Moss Point School District

The Moss Point School District Located in Moss Point, Mississippi, deployed a video surveillance solution to monitor its ten schools and district offices. [28] The School District serves 3100 students in a high school, junior high, and six elementary schools. The district has 250 teachers and 30 administrators. The district's current security scheme consisted of a few schools having analog video surveillance systems.

When the school district decided to upgrade their video surveillance systems, the district established two important requirements for a new video surveillance solution. It had to work with the schools' existing analog video surveillance cameras and later it would need to integrate with other physical security systems, such as access controls and alarms. Moss Point School District already had a Cisco IP network infrastructure, which is why they decided to use Cisco for their new physical security system. "We didn't want to buy separate monitoring and control systems for our video cameras, HVAC [heating, ventilation, and air conditioning], access controls, and intercom systems," says James Glover, chief information officer of the Moss Point School District. He continued "Only the Cisco physical security solution lets us control all of these systems from a single interface."

For help with planning and implementing the solution, the district turned to Coleman Technologies, a Cisco Gold Certified Partner. Coleman Technologies first conducted a site evaluation of each school and met with district administrators and school principals to identify the locations that they wanted to monitor. Before the fall semester of 2008, Coleman Technologies installed more than 200 cameras with enclosures to protect them from tampering in the district's 10 facilities. Most were installed in the hallways and campus perimeter, a few in classrooms. Eventually, the district will install a surveillance camera in every classroom.

The next stage of the project was to enable centralized monitoring of all video surveillance cameras on all campuses. To accomplish this, Coleman Technologies installed a Cisco Metro Ethernet solution to interconnect all of the district's campuses. This allowed video streams from each school to travel to the central office at the high school. Campus security personnel can then monitor it using Cisco Video Surveillance Operations manager. Security personnel will be able to control which video feeds are pushed to principals' monitors using Cisco Video Surveillance Virtual Matrix. The district superintendent will be able to monitor video streams from all campuses.

[28] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9145/ps9152/case_study_c36-508965.pdf

Using Cisco's Physical Security Solutions gives the Moss Point School District the foundation needed to expand the system. The Moss Point School District will add the IP cameras to all class rooms and it will add physical access control gateways to integrate their current systems.

Cisco Products Used

Switching and Routing

● Cisco Integrated Services Router
It allows customers to consolidate costly branch-office servers and deploy new applications centrally, while offering real-time access to physical security video and data.

Physical Security

● Cisco Video Surveillance Media Server:
The Cisco Video Surveillance Media Server manages, replicates, distributes, and archives the video streams.

● Cisco Video Surveillance Operations Manager:
It enables organizations to quickly configure and effectively manage complex video applications throughout the enterprise. It meets the diverse needs of administrators and operators by providing multiple Web-based consoles to configure, manage, display, and control video throughout a customer's IP network.

● Cisco Video Surveillance Virtual Matrix:
The matrix allows any operator or integrated application to control what video is displayed on any number of physical and virtual monitors, both local and remote. It uses the IP network to provide aggregation and transmission of video from cameras and recording platforms much like the function of a classic analog video matrix switch.

The price for the physical security components used estimate to:
IP Cameras, 200 @ $1,000 per plus installation costs
Media Server, $1990 per server
Virtual Matrix, $2,450 per matrix
Operations Manager, $4960

Total price for the project would have to be in the high six figures, the ABC Security project on the next page was quoted around $300,000 at about one third the size of this project.

Unified Communications

● Cisco Unified Communications Manager:
Cisco Unified Communications Manager is an enterprise-class IP telephony call-processing system that provides traditional telephony features as well as advanced capabilities, such as mobility, presence, preference, and rich conferencing services.

● Cisco Unified IP Phones:
The Cisco Unified IP Phones unifies voice, video, data, and mobile applications on fixed and mobile networks. These applications use the network as the platform to enhance comparative advantage by accelerating decision time and reducing transaction time

● Cisco Unified MeetingPlace:
Cisco Unified MeetingPlace lets you incorporate multiparty discussions and application sharing into a broad range of communication scenarios. This solution integrates audio, video, and web conferencing capabilities to give remote meetings a natural and effective in-person quality. It allows Conferencing traffic runs over your organization's IP networks to reduce toll charges and recurring conferencing fees. You can isolate confidential meetings behind the firewall to enhance security, while also having the flexibility to set up Internet-accessible meetings with external parties.

ABC Security Credit Union Integration Project

The next case study I will discuss relates to a project conducted by ABC Security. ABC Security is Sentry Security's, enterprise-level security division. I'm a service technician at Sentry Security. Sentry Security, along with ABC Security, is a provider of security solutions for homeowners, small businesses, and large enterprises. We specialize in the installation, service, and monitoring of security and fire alarm systems, as well as access control and video surveillance. This project consisted of installing Access Control, Video Surveillance, and Burglar Alarm systems at a Chicago land Credit Union. The name of the Credit Union will remain anonymous due to confidentiality reasons. The project was conducted in 2007 with a project price around $300,000.

Access Control System:

The access control system consisted of equipment manufactured by S2 Corporation.[29] The equipment is completely integrated with the video surveillance and burglar alarm systems. Input and output modules were installed so that alarm conditions trigger the appropriate camera recording and automatic call up, as well as provide off-site central station monitoring of selected points. The integration between the S2 access control system and the ON-SSI video system used

[29] http://www.s2sys.com/

in the project is network based and may be programmed or modified by the local administrator. The local administrator controls the programming and operation of card readers, access levels, user permissions and access rights. Full relational database historical transaction reporting is included along with the ability to create and save report templates.

The proximity card readers used for this project are HID Multi-Class readers[30]. These readers read at the organization's current 125 kHz proximity credentials. The readers provide a more secure, longer bit, 125 kHz proximity credential. This reader will permit migration to HID I-Class, ISO 15693 Smart cards or MIFARE Smart card technology, as well as government FIPS format without changing out the readers. One 125 kHz technology credential and one smart card technology credential may be read simultaneously so that future smart card migration can be easily phased in over time.

All card-reader-controlled doors have door position monitoring and request-to-exit functionality. This functionality enables doors to report both door forced open and door propped open conditions. The card readers will indicate access granted or denied and if denied, the reason for denial. Some doors were installed with IN/OUT readers; this set up permits the doors to be set for anti-pass back protection. Anti-pass back prevents re-entry in the same direction if a valid access is not recorded in the alternate direction. Pass-back violations may cause a physical lockout of doors or violations may be reported as alarm conditions only without the physical lock out.

All alarm conditions may be mapped to graphical map displays and selected video cameras for alarm assessment and disposition, or for historical forensic analysis. Manual operation of the access control system may be done directly through graphic map displays via pre-programmed icons.

The S2 system is administered through a standard Web browser such as MS Internet Explorer; this eliminates the need for client software. The system may reside on the BCU network without using the CITRIX server for client access.

Video Surveillance System:

The surveillance system utilizes a NET-DVMS network video recording system manufactured by On-Net Surveillance Systems Inc. (ON-SSI).[31], IP Cameras manufactured by ACTi Corporation[32] and IP video conversion solutions manufactured by Axis Communications.[33] For scalability, camera vendors may be interchanged in the future since the ON-SSI Network Video Recording system is compatible with a wide range of manufacturers' cameras.

[30] http://www.hidglobal.com/
[31] http://www.onssi.com/
[32] http://www.acti.com/
[33] http://www.axis.com/

The video surveillance and recording system is an IP-based system. All interior IP video cameras installed were connected via PoE. Analog cameras are connected to the network using IP converters. To integrate the access and video technologies, NET DVMS Software with a two-way interface license were installed.

Outdoor vandal-resistant cameras with heaters were installed and connected via UTP conversion through a low-voltage mid-span power supply at a network switch. The UTP conversion is used to physically eliminate the possibility of the Credit Union's network from being accessed from outside of the secured building.

The network-based system utilizes the customer's network for video transmission to a central Network Video Recording (NVR) server. This server retains the data for service center cameras for a minimum of 90 days and all other building cameras for 30 days.

Two physical servers were installed with long-term archive storage drive array to implement the system. The Service Center camera server required a storage drive capacity of 2.2TB for 90 days of archive storage. The remaining building cameras required a server with either 2.0TB for 30 days or 3.0 TB for 45 days of archive storage. Additional archive storage may be added as needed to increase the system archive capacity or to accommodate additional cameras.

Burglar Alarm System:

The burglar alarm system installed is an Underwriter Laboratory (UL listed) commercial alarm system using both a standard dialer line and a GSM radio backup transmitter. The alarm control panel is a DMP XR-500 system with 7070 alphanumeric display keypads.[34] The burglar alarm system is divided into three areas, the service center, the branch area, and the vault. Alarm devices are listed in the access control door schedule and the Service Center alarm zone schedule. Alarm conditions generated by card reader-controlled doors not in the Service Center, are connected through the S2 access control system outputs to the burglar alarm system for off-site monitoring. Alarm conditions generated by the Service Center burglar alarm panel are connected to the S2 access control system for integration with the video surveillance system camera call up and for local on-site monitoring notification.

Special hold-up alarm operational features include auto-door relock of the service center and selected perimeter doors to prevent a perpetrator from re-entering the building. The elevator will also be activated into Fire Recall mode so that it will return to the 1st floor and be unable to be used to access the upper floors. Local visual indicator lights in office areas outside of the service center will be activated to warn on-site personnel that the hold-up alarm has been activated. A special switch or keyboard command can be used to lock out the service center card readers during an incident investigation so that only authorized personnel may enter the Service Center.

[34] http://www.dmp.com/

CONVERGENCE

ABC Security has been integrating access control and video system for several years now. This project has given the Credit Union the infrastructure to expand the system and further integrate the IT technology with their physical security. I will list the major components of this integration project on the next page.

Product List:

1. S2 NetBox:
The S2 NetBox access control system offers a full-featured, credential-based access control program running on a snetwork appliance platform. Its architecture is fully distributed, with a complete database maintained on the S2 Network Controller (S2NC) and relevant data

distributed to the S2 Network Nodes (S2NNs), assuring that the access control capability survives network outages. The access control facility integrates fully with the optional Identity Management Solution for ID photo capture and badge generation as well as with the Video Management System for access transaction recording and replay. Integration with common alarm panels includes such features as system disarm on valid access by selected people and access privileges that are enabled when a building alarm system is disarmed.

2. OnSSI, NetDVMS:
NetDVMS is OnSSI's market-leading multi-site, multi-server enterprise-scale network video recorder and camera management platform. NetDVMS provides automated event detection and intelligent video delivery through integration with physical security systems and advanced content analytics. OnSSI's open-architecture technology allows for seamless convergence with security, retail and other organizational systems. Simple-to-use APIs enables integrating NetDVMS with Access Control, Contact Closure, Fire Alarm Panels, Emergency Phones and most other IP-based systems, to create a true alarm, alert and event management system.

3. ACTi IP Cameras:
ACTi IP camera can compress and transmit real time images with outstanding image quality (VGA, 640x480) at reasonable bandwidth through a standard TCP/IP network. The cameras used were Ethernet ready and have the powerful ARM9 SoC with excellent system performance to offer dual streams of MPEG4/MJPEG, and both formats offer megapixel resolution.

4. Axis Communications Video Encoders:
A video encoder digitizes analog video signals and sends digital images directly over an IP network, such as a LAN, intranet or Internet. It essentially turns an analog video system into a network video system and enables users to view live images using a Web browser or video management software on any local or remote computer on a network.

5. HUD Multi-Class Readers:
The multiCLASS product line give the ability to use existing cards, deploy multi-technology cards and transition to new contactless smart card technology without having to change the access control system card holder database. With multiCLASS, customers are able to transition to contactless smart cards over time while incorporating the use of multiple card technologies within a single building or across multiple facilities.

6. DMP-XR500 Burglar System:
The XR500 Command Processor Panel has 574 inputs, 16 doors of access, 502 Form C relays, 32 areas, and 10,000 users. It communicates via the network or digital dialer.

CONCLUSION:

The convergence of physical and IT security is a growing trend in organizations that will continue to grow across the United States and countries across the world. This process will deliver benefits to organizations like reducing costs, increase efficiencies, risk management, and compliance. The current state of the economy is forcing organizations to analyze their current business operations and find ways to reduce costs. Organizations are shifting to a more holistic security infrastructure and convergence will accomplish this process.

The convergence process is a complex endeavor that requires detailed research and planning. Convergence of these two technologies does not just mean integrating hardware components, it means implementing a change in organizational structure. A truly converged physical and logical access security solution should consolidate identities, set policies, monitor and track events, manage user access rights to software applications and generate consolidated reports. Every organization will have different goals for their security infrastructure, so the strategy they use to converge will be different. In this paper I have introduce different strategies to converge. These strategies were created and have been implemented successfully by well known organizations like the Open Security Exchange (OSE) and Microsoft Inc. These strategies can be used as guidelines for an organization to use in their implementations of the convergence process.

REFERENCES:

1. Cisco Expands Physical Security Solution Portfolio, LAS VEGAS, ISC West - April 2, 2008
http://newsroom.cisco.com/dlls/2008/prod_040208.html

2. http://www.cisco.com/web/solutions/ps/products.html

3. http://www.cisco.com/en/US/products/ps6712/index.html

4. http://en.wikipedia.org/wiki/Storage_area_network

5. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/ch-raid-intro.html

6. http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps6921/ps6936/product_data_sheet0900aecd804a3e6d.html

7. http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9145/ps9151/prod_brochure0900aecd806e9870.pdf

8. http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ ps9145/ps.9152/case_study_c36-508965.pdf

9. http://www.sans.org/reading_room/whitepapers/authentication/convergence_of_logical_and_physical_security_1308?show=1308.php&cat=authentication

10. Analysis: Physical/Logical Security Convergence, by Jeff Forristal on November 17, 2006
http://www.networkcomputing.com/print_entry.php?eid=61439

11. http://www.scaleoutadvantage.techweb.com/news/fut_nwc20061123_Physical.jhtml

12. http://www.infosectoday.com/Articles/convergence.htm

13. download.microsoft.com/download/5/f/e/.../PhysicalSecurityTWP.doc

REFERENCES:

14. http://www.istonline.com/pdfs/white-papers/ose_physical_and_it_security_convergence.pdf

15. The Open Security Exchange (OSE) Convergence Roadmap, Copyright ®2007-08 OSE

Quantum Secure, Inc. Vik Ghai, Laurie Aaron. HID/Fargo Gary Klinefelter, Greg Sarrail

Koffel Associates Shayne Bates.

http://www.theose.org/uploads/Convergence_Roadmap_2008-v1.0.pdf.

16. Physical Logical Security Convergence and What it Can Mean to Your Business,
By: David Ting posted: Sep 15th, 2009
http://www.articlesbase.com/print/1234839

17. Convergence of Logical and Physical Security
Yahya Mehdizadeh GIAC GSEC Certification October 14th, 2003
http://www.sans.org/reading_room/whitepapers/authentication/convergence_of_logical_and_physical_s ecurity_1308

18. Combining Cyber and Physical Security
Frank Madren, GarrettCom -- Control Engineering, 4/1/2008
http://www.controleng.com/article/271143-Combining_Cyber_and_Physical_Security.php?rssid= 20307&q=combining+cyber+and+physical+security

19. http://www.surveillance-video.com/vidtranovin.html

21. Converging Security Technologies, by Michael Fickes
http://web.kennesaw.edu/news/stories/converging-security-technologies

22. http://hspd12.usda.gov/about.html

23. http://www.cac.mil/assets/pdfs/DEPSECDEF_Policy.pdf

24. http://www.s2sys.com

25. http://www.onssi.com

26. http://www.hidglobal.com

27. http://www.acti.com

28 http://www.axis.com

29. http://www.dmp.com