Why Integrate Physical and Logical Security?

Last Updated: June 11, 2011

Solution Author

John Carney

John Carney, Senior Manager, CMO Industry Solutions Engineering, Cisco Systems

John is a senior technical market manager in the Central Marketing Organization supporting the Public Sector market segment in the areas of Government and Security. He joined Cisco in January of 2007 and has served as an Industry Solution Architect responsible for the design and validation of solutions focused on the Healthcare, Financial Services, and Public Sector verticals. With over 25 years experience working in a service provider/data center environment, John's strength lies in his unique ability to understand the business issues facing our customers and how they relate to the components in a large computing environment. Security and the challenges of integrating security solutions have been a focus for John for many years.

To provide feedback on this document or obtain additional information, please contact the author directly at johncarn@cisco.com or via phone at 610-695-6211.

CONTENTS

Convergence of Physical and Cybersecurity 1

Overview 2

Securing the Network 3

- Outside–In 3
- Inside–Out 4
- Inside 4
- A Possible Solution 5

Protecting the People 5

- A Possible Solution 6

Securing the Data 6

- A Possible Solution 7

Securing the Facility 7

- A Possible Solution 8

Conclusion 8

Why Integrate Physical and Logical Security?

This document is the first in a series of papers from Cisco that addresses a variety of topics that are of interest to members of the government agencies, both public and private sector. The document describes the importance of integrating physical and logical security under a single governing body or department. Subsequent papers will discuss specific points of integration to address business challenges in the market.

This is not intended to be a how-to document, but rather to provide new perspectives on security, security management, and device integration. Future papers will discuss the business challenges created by security silos, and specific products and integration solutions to address those challenges.

Convergence of Physical and Cybersecurity

Despite the fact that physical and logical security depend on each other, it is surprising to find that a number of companies still treat them as separate systems, from both a device management and government agencies perspective. Until recently, this was justified because the technology to integrate physical and logical security was not yet available.

Regarding security, most organizations have at least three buying and control centers. The first two are primarily concerned with IP theft, malware, viruses, and so on: NetOps handles network security, while InfoSec manages data at rest and data in transit security. The third is physical security, which includes surveillance and access control. In most organizations, the guard at the gates is a separate operations center.

Today, more than ever, the problem comes down to governance, making it a priority to create a single body for security policies, procedures, and deployments.

According to Scott Borg, Director of the U.S. Cyber Consequences Unit:

"*As long as organizations treat their physical and cyber domains as separate, there is little hope of securing either one. The convergence of cyber and physical security has already occurred at the technical level. It is long overdue at the organizational level.*"
(http://fedtechmagazine.com/article.asp?item_id=512)

This comment highlights the fact that physical and logical security technologies have matured to the point that they can now be integrated. The convergence of the IP network and the migration of legacy sensors and appliances to TCP/IP have helped drive this transformation. Cameras are now IP-based; card readers use the IP network instead of a proprietary network; and access lists, policies, and procedures

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

are stored and generated by computers. Additionally, consider security standards such as Payment Card Industry (PCI), likely one of the most advanced security policies available. This governing body includes both physical and logical security in the policy, as do others.

Cybersecurity, meanwhile, depends greatly on physical security. Attackers who can gain physical access to a computer can almost always take advantage of that access to further their efforts. Merely getting access to a physical terminal where a memory device can be plugged in is usually sufficient. Any device present that is connected to the network must be protected to ensure that it cannot be turned into a tool to be used in an attack.

The lack of integration between physical and cybersecurity creates the following challenges:

- No single system to identify a person's identity because each functional security department controls its own identity database
- Increased potential for theft
- Lack of IT management and application of best practices applied to physical security devices, or a lack of best practices applied consistently across departments or organizations
- Lack of physical monitoring of logical security devices that can detect tampering; that is, unauthorized access to a logical security device console

Overview

Today, *security* can mean either physical security, as in physical access control, or logical security (also known as cybersecurity), as in virus detection or unauthorized network access. The departments that manage the technology for these two types of security are usually entirely separate, and often do not even collaborate. With the proliferation of IP convergence on the network, this can have a dramatic impact on both departments, as well as the safety and security of an organization.

This document describes the background and future trends of logical and physical security management; why the two departments need to collaborate, and why having a solid network foundation is critical to a solid security posture.

A solid security policy starts at the top. Having a single, high-level individual or department responsible for a comprehensive security policy, whether actual or virtual, that covers both physical and logical security is paramount. Having executive sponsorship (such as CIO, CSO, and so on) as the governing body with cross-functional or cross-departmental teams for the requirements gathering and policy definition ensures that the various department-specific requirements are taken into account. Developing the security policy in silos hinders the ability to effectively deploy these policies.

Before the convergence of applications, devices, and services onto the IP network, security measures were largely separated:

- Video surveillance ran across dedicated analog connections.
- Physical access to buildings was managed entirely across an isolated network instead of the LAN, as it does today.
- Intrusion prevention was done at the firewall.
- Virus scanning and intrusion detection was done on the desktops.
- E-mail (spam) and web security (acceptable use policies) were limited to users within the organization boundaries only. The risk was that an employee could bring in an infection from outside.

The convergence of voice/video/data has brought the following changes to each of these areas:

- Voice (a.k.a. audio)—In addition to traffic created by deploying voice-over-IP (VoIP) services, *voice* now refers to other audio sources, such as crowd monitoring, a gunshot in a high crime area, or noise detection in a building that is supposed to be vacant (for example, during the night).
- Video—In addition to video calls, video chat sessions, and teleconferencing, *video* now also refers to video surveillance, traffic cameras, digital signage, and streaming video.
- Data—Access to *data* is not just in the intranet anymore; with the explosion of cloud services, access to data can be anywhere, anytime from any device.
- Network—Multiple heterogeneous devices are connecting to the network, such as smartphones with video, personal laptops, and so on. There is little distinction between a device and its uses for a particular purpose only.
- Social media and enterprise collaboration also play a role in reporting security incidents, thus requiring the analysis of all sorts of data within the organization.

According to IMS Research, which tracks the installed base of Internet-capable equipment, the number of devices connected to the Internet passed the 5 billion milestone in 2010, and this number is expected to reach 22 billion by 2020. This surge reflects the explosion of personal devices such as smartphones and tablet computers, and also includes all the sensors, cameras, and devices used in security that are now IP-enabled because of the convergence of the IP network.

This massive convergence can have a negative impact on the performance of the network if the network has not been properly designed and deployed to handle this increase in traffic. Along with presenting new security challenges, the convergence of Internet-connected devices, voice, video, and data also provides ways to integrate logical and physical security that were not possible just a few years ago.

The following sections explain how linking physical and logical security streamlines management, reduces costs, and provides maximum security to the enterprise.

Securing the Network

"The critical infrastructure is in play," Black Hat founder Jeff Moss said recently in opening the annual Black Hat Federal cybersecurity conference. "If your assets are in play, you'd better be able to respond and recover faster."
(http://gcn.com/articles/2011/01/21/cybereye-infrastructure-resliliency.aspx?s=gcndaily_240111)

A compromised network allows access not only to business-critical data, but also to all of the security sensors, video cameras, and access controls. Unauthorized access to a single security sensor such as a video surveillance camera can be bothersome, but compromising the control of all sensors can be disastrous. Many technologies are available to secure the network against the wide variety of threats that exist.

Outside–In

One of the most important ways to secure the network is from the outside–in. The most secure network is one that is not connected beyond itself. However, because this does not allow users to collaborate outside of their specific location, firewalls are commonly used to prevent unauthorized access to the production network. This is an effective way to manage outside access to the network, but with the prevalence of wireless networks these days, it is only a partial solution.

Wireless networks that allow access from outside the physical plant to the production network environment present another security challenge. Measures such as hiding the SSID to prevent the advertising of the network and using 802.1X security protocols to prevent unauthorized connections are helpful but not always sufficient. Depending on the protocols and encryptions methods used, you still leave the potential for a brute force attack on your network.

With the rise in social networking, brute force attacks against the network are much easier because of the amount of information available. You can likely glean the company, department, project, username, and possible passwords for an individual just by browsing their social networking accounts.

Consider the following scenario:

- An employee has an account with a social networking site, listing their name.
- That employee happens to post a picture from a team building event, stating “Here is a picture taken with my co-workers from *XYZ* company”.
- That same person posts pictures of their pets, children, spouse, and so on, and happens to also post the name of the pet or persons listed.

Malicious hackers know that many people use their pet, spouse, or child’s name as part or all of their passwords. With this information readily available, it is far easier to guess passwords than it used to be.

When an authorized user’s credentials have been compromised, the firewall does not stop an intruder with a valid ID and password. One possible solution is to deny access to the production network unless the individual has identified himself or herself to the facility. In other words, deny access to the network resources from any device unless the user has been granted access via a card reader on the premises (security from the outside–in). Assuming that there are separate VLANs set up for guest and production access, this would not prevent a user from accessing the network outside when moving between buildings, because they would remain connected to the production network once authenticated. In addition, this provides a higher degree of secure access for the wired and wireless network. If users need access to the production network before entering the building, they can access the guest wireless network and use VPN access from their laptop.

Inside–Out

If unauthorized access to a company network results in a crime being committed using that connection, the company shares the responsibility. This is an additional incentive for eliminating unauthorized access to a private network.

An obvious strategy is to limit access to the building; an extra layer of security is provided by limiting access to the network if the user has not swiped their badge. This deters unauthorized individuals from accessing the network by attempting to login to an unattended computer if they do gain entry into the building. From a policy perspective, you could extend this method to allow access to assets only if the individual is accessing them from a terminal they are registered to use, which means an intruder would not only need to have credentials, but also know the computer the credentials were allowed to use.

Users with access to the network need to be protected when they navigate outside of the intranet, which requires a solid foundation of network, access, and privacy tools. It’s a good practice to ensure that employees are not accessing known hacker sites or bringing unwanted probes into the network. Most of this protection can be accomplished at the network layer with the proper security appliances in place, and then augmented at the individual user stations with virus protection and scanning software.

Inside

Most security attacks occur from the inside. Many hardware and software tools are available to help keep data secure, but two factors are critical: developing a sound security policy, and ensuring that the network can effectively implement and enforce those policies.

If web-acceptable use policies are not in place, employees may go to malicious websites knowingly or unknowingly (phishing attacks) and download Trojans, keystroke loggers, and so on; thus revealing confidential network information to the hacker. Similarly, employees with laptops at home are beyond the corporate policy, and are thus able to download any content and bring it back to the office. These behaviors need to be prevented by ubiquitous policy inside and outside the organization.

Another way possible with the integration of logical and physical security is to track computer and data access as well as location. For instance, there may be valid instances where a user who has swiped a badge in Singapore needs to access a computer in Chicago, but this would usually be an indication of suspicious behavior that should be tracked. Creating a universal notion of location across physical, network, and logical domains makes it easier for customers to use that information across their entire policy definition effort.

The bottom line is, take the time necessary to create the appropriate security policies. Understand the level of security you want to implement, what you want to secure, what tools are available from a security and policy perspective, and make sure that your network can handle the stresses of the tools. The best policies in the world are worthless if the network resources cannot access them in a timely fashion to enforce them.

A Possible Solution

“In an open, trusting and tech savvy environment, the best access control system may be predicated upon a link to system access. If you fail to badge into the building, you don’t get access to the systems. The collateral benefits abound: building managements systems, incident awareness, and who is in the affected building.” Edward Erickson, Senior Director of Safety & Security, Cisco Security and Business Resiliency (SSBR)

A high impact solution that has minimal impact on the human engineering side is to ensure that only trusted users access the network. To enforce this, require a user to badge into their building prior to being able to access the network. The user does not have to change their behavior of swiping a badge in front of a reader, or how they log in to the network. However, this now creates a multi-factor authentication: something you *have* (a security badge), and something you *know* (your ID and password). By tying building access to network access, you increase the security of not only your network, but your network resources as well.

Using multi-factor authentication, gaining entrance to the building no longer guarantees access to the network, which makes it more difficult for an unauthorized person to take advantage of an unattended computer. This also addresses the common issue called tailgating, where one person follows another into a building without swiping their badge across the reader. From a safety perspective, this can cause problems in an emergency case, because the number and names of the people in the building are not known. Requiring a badge swipe provides the following security benefits:

- Provides information on who entered the building.
- Eliminates tailgating since the network cannot be accessed without the person swiping his/her badge.
- Allows for a more productive work environment by making it easier for the employee to authenticate by using an integrated solution

From a social engineering perspective, badge use has minimal impact on people because most already swipe their badge for access to buildings. All that is required is to make the practice mandatory.

Protecting the People

Protecting the people involves a combination of physical and logical security. Physical security keeps them safe by allowing only authorized individuals into the building. Logical security protects their computers and data from unauthorized access.

Identity management, the administrative area that deals with identifying individuals in a system, is likely one of the most important design considerations made in an overall security strategy. Being able to trust the identity of your users makes the job of managing their identities that much easier.

The physical security team must track all users; to which areas they are allowed access, when they are allowed to access those areas, and so on. The logical security team must track those same users; which computers and servers they use, data access rules, and so on. Combining these two administrative functions into a single system allows for a more efficient change management process and minimizes the potential for an out-of-sync situation between systems.

Both physical and logical security play a role in identity management. Having two distinct systems to manage the identity of a single individual creates a potential for an out-of-sync situation. For example, consider the case of an employee termination of employment. With multiple disparate systems, it is not uncommon for the termination of an employee across all systems to have a time lag, thereby creating a potential security threat.

Combining logical and physical identity management does create challenges, however. This is where the concept of a single governance body for security becomes vital. This governance body needs to determine who can make changes, what changes they are allowed to make, and when they can make them. Keeping the identity data accurate needs to be a priority because all policies and procedures use this data to enforce the policies that have been created.

Now that you know who your employees are, you need to ensure that you keep them safe. When an accident or dangerous situation arises, you need to be able to effectively notify the people in the building and direct them away from the danger.

A Possible Solution

Both physical and logical security groups are required to maintain various roles and rule-based access. Areas such as distributed security administration, policy administration, and access control are included in both types of security. However, most companies currently have two completely separate data stores controlling access. Combining these in a common identity management system not only increases security by minimizing the impact on change management, but also saves costs in terms of compute cycles, storage, and manpower when a change request occurs. For example, with a common identity management system, employee termination of employment can be done cleanly across the entire policy space.

Once you are confident you know the identity of your employees, it is imperative to keep them safe. Consider a scenario in which a fire detection/suppression system is integrated with a video surveillance system. Knowing the location of a smoke detector that has been triggered allows the facility to provide a safe egress route away from the area where smoke was detected. It can also provide a way to trigger the video surveillance system to retain the recorded information from cameras in that area for a period before and after the incident for analysis. Further, understanding the location of the fire allows for an

automated message via public address or over the IP telephones and digital media suggesting the safest evacuation route. Having this information available and automated allows for faster reaction times for evacuation, and can also provide advance information to the first responders.

By integrating physical and logical security systems, you can more effectively manage, maintain access, and notify the occupants of a building in case of an emergency. Being able to automate that process allows for a more efficient transfer of information between systems and occupants, and minimizes the potential for false positives.

Additionally, the implementation of a centralized threat operations center that continuously monitors the feeds coming in from IPS sensors, e-mail and web attacks, and can correlate various kinds of attacks to blacklist IP addresses from where the attacks originate, can have a positive impact on the overall security posture of a company. This way, the technology can provide real-time protection to networks across the globe by sensing an attack coming from anywhere around the world.

Securing the Data

Securing the data involves more than simply database access. Data comes in many forms; most organizations have not only private data, but intellectual property, which can come in the form of patent applications and source code, internal presentations, development plans, and even employees' memories. Developing a security plan that takes all these disparate types of data into account involves more than just physical access to the computer room or access to the network. You also have to prevent unauthorized access to data by employees or others, as well as monitoring attempts to do so.

An often overlooked scenario, particularly in the case of security data, is assessing the user's asset that is used to access the data. Making sure the asset is managed and has the appropriate safeguards on it to download and store sensitive data (antivirus, disk encryption, and so on) can be a powerful method of determining access.

A Possible Solution

Keeping all of the data in a single location with a single system to manage access simplifies the physical and logical policy deployment. With the convergence of the data center space, all the data is now being stored in single or multiple-connected environments. This simplifies the policies, at least from a physical access perspective.

Included in this huge data warehouse are not only the business-specific data, but also the security-related data, such as the access control database, video surveillance archives, virus definition files, and so on. Keeping the security data safe is as important as the business data. An unauthorized user who gains access to the security data archives could conceivably erase any indication of a security breach.

This is another case where physical and logical access used together can create a more secure environment. Requiring system administrators to identify themselves at the physical entrance before being allowed to access the console can prevent users who are authorized to access the physical space from using another user's credentials to access systems to which they themselves do not have access, which is one of the more common ways that internal security breaches occur.

Securing the Facility

Although securing the facility is typically considered a physical security function, the wireless network now extends the "virtual" facility outside the walls of the physical space. In the past, gaining access to the network required that you be inside the physical location. This is no longer the case because the wireless network extends the access to outside the building or the logical building space. Being careful to secure the logical facility is just as important as securing the physical facility.

Now that the logical access to the network extends outside the building, you need a way to effectively monitor for and manage potential security threats. Consider the case where a hacker drives past a location looking for open access points. Being able to identify both the threat and the individual is necessary to prevent the attack, as well as possibly prosecuting the individual.

You should not only consider physical and logical security in securing the facility, but how you use the information collected. For instance, do you really want to allow lights to be turned on or certain floors of the building to be accessed when nobody is on-site? Or, would there be a reason to deny access into certain areas when a supervisor is not present?

When multiple departments or agencies share a single building (as is the case in many government buildings), the costs of duplicating the infrastructure for every department or agency, including the server room, data stores, and network infrastructure, can be enormous. Finding a way to securely share the infrastructure is best from a cost perspective, but is it safe?

A Possible Solution

By tracking a user's identity, you can apply rules that identify roles and responsibilities for that user. This is not only useful for data access policies, but can be used for functions relating to building controls. People entering the building after normal hours can either be authorized or not permitted to perform functions such as turning on the lights, or raising or lowering the thermostat. You can further restrict access to specific locations, allow the elevator to stop only on a particular floor or floors, or track who is in the building, as well as create policies that prevent access if the right combination of personnel is not present. Having all of this information in a single store helps simplify the integration of the systems by providing a core data store so that all policies use the same identity information.

Monitoring the logical plant and using the physical security infrastructure can also help discover malicious threats. By monitoring the wireless network for potential unauthorized access, you can trigger the video surveillance system to retain the video from the area where the attempt was made. Adding video analytics automates the comparison of the vehicles or persons in the area when a possible breach occurs. Even without video analytics, having the video archived automatically allows for a more complete forensics analysis if a breach occurs.

There is a network component to securing the facility as well. Installing multiple physical networks and server rooms is not cost-effective. By creating virtual networks over the same physical plant, you can effectively isolate the departments from each other without compromising the security of each. Creating policies that allow individuals to access only the virtual networks that they have authority to use is a way to maintain the security of the network without incurring the costs of duplication. In addition, with virtualization and cloud technologies becoming more mainstream, this provides an easy way to deploy these technologies without having to perform a "forklift upgrade".

Conclusion

A sound security posture must be designed holistically. Having a single governance team, organization, or cross-departmental virtual team accountable for the overall design of the policies and procedures helps ensure that the needs of all stakeholders are met and that the deployment allows for the flexibility to manage across silos without negatively impacting the ability to create the desired security posture.

The integration of physical and logical security domains allows you to better secure your assets. When you decide to integrate the logical and physical security domains, ask yourself the following:

- What are you trying to protect?
- Where is it located?
- How do you build security around it?

Combining your logical and physical security processes and infrastructures simplifies the manageability of the security infrastructure and increases visibility to your resources, which makes it easier to detect and prevent security incidents, and provides a platform to manage the response and recovery after an incident occurs.

By using a common identity manager, you can trust that you know the person presenting credentials across the organization. By deploying an identity validation solution that includes network admission control, you create a multi-factor authentication deployment with minimal impact on the current work habits of your workers.

In summary, the integration of physical and logical security can provide the following tangible benefits:

- Creates operational efficiencies
- Reduces risks and improves risk management
- Provides better, more streamlined incident management when breaches occur
- Maximizes existing investments
- Reduces operation and management costs

There are many more opportunities to integrate physical and logical security than presented in this document. Once you start looking, you will very likely see administrative redundancy as well as security opportunities that can be enhanced by combining these two sets of technologies.