5-2008

Convergence of Physical and Logical Security: A Pre-implementation Checklist

Juan C. Melendez
Iowa State University, juan@juanmelendez.net

Andy Luse
Iowa State University, andyluse@iastate.edu

Anthony M. Townsend
Iowa State University, amt@iastate.edu

Brian Mennecke
Iowa State University, mennecke@iastate.edu

Convergence of Physical and Logical Security: A Pre-implementation Checklist

Juan C. Meléndez
Iowa State University – Graduate
juan@juanmelendez.net

Andy Luse
Iowa State University
andyluse@iastate.edu

Anthony M. Townsend
Iowa State University
amt@iastate.edu

Brian Mennecke
Iowa State University
mennecke@iastate.edu

ABSTRACT

Physical and logical security within an organization have traditionally been implemented and administered as separate standalone entities. A growing number of companies are integrating these two systems to provide greater security along with lower cost and time requirements for administration. The following paper provides an overview of security convergence, including standards and initiatives driving this movement. A pre-implementation checklist is then provided as a template for those who wish to prepare themselves for a convergence project.

KEYWORDS

convergence, physical security, logical security

INTRODUCTION

Physical security operations focus on the protection of tangible assets reinforced by security guards and complex lockdown operations in an organization. Information security also known as computer security or cyber security is a much newer area that focuses on the protection of information systems and digital assets of the organization (Whitman 2003; Hoffman 2006; Mehdizadeh 2004). In most organizations, physical security operates independently from information security and even though both entities work for a common goal they are operated and managed as their own entity. Consequently, organizations struggle on a daily basis to keep a proactive approach in protecting themselves from security threats, losing in this way control over their security operations. As a result, a new concept that merges the physical and information security operations has emerged in order to fill in the gaps from these two security environments. This concept is known as Security Convergence (Contos et. al. 2007)

An issue often overlooked regarding security convergence is the complexity of preparing these environments for convergence deployment. Many manuscripts provide information regarding technologies available, standards used, and tips for successful deployment (Kinslow 2006), but few offer advice for readying for organizational implementation. While deploying the technology is important, preparatory steps are also critical to the success of the system.

The rest of this manuscript is organized as follows. An explanation of *Security Convergence* is given and prior researched discussed. Next, *Standards and Initiatives* for security convergence are explained. A *Pre-Implementation Checklist* for organizations is then described for those who wish to ready themselves for a security convergence project. Finally, *Conclusions* are discussed.

SECURITY CONVERGENCE

According to a survey conducted by PricewaterhouseCoopers and CIO Magazine in 2005, 53% of organizations have achieved some level of integration between their physical and information technology security operations, an increase from 29% in 2003 (Hoffman 2006). This is a clear indication that organizations are closely paying attention to this initiative and acting upon it.

The rapid expansion of the enterprise's ecosystem is a phenomenon with a cascading effect from the business operational units down to the IT infrastructure and, therefore, to the security operations. The increase in global operations and the metamorphosis of business processes has triggered an increase in information assets and a rise in digital dependence. In addition, new regulatory practices and compliance regimes put an even greater burden on the organization's IT security resources, increasing its dependence on technological solutions. As a result, IT managers are desperately seeking ways to enhance their organization's security environment while keeping costs low (Booz Allen Hamilton 2005). For the last several years, organizations have observed an increase in their security spending, as security operations in enterprises have gotten bigger and security threats have risen. The integration of security systems offers the benefit of reducing the overhead cost of the security operations by providing a more controlled environment and increasing its efficiency (Mehdizadeh 2003).

The process of implementing a holistic security system involves the integration of the security technologies in addition to the integration of the security management processes. According to Mehdizadeh from the SANS Institute, both are equally imperative (2003). Many security technologies have emerged over the years to help manage and mitigate security risks. These, however, operate independently and do not communicate with each other.

The scope for the convergence of physical and logical security can be divided into three primary areas (Bernard, 2006):

1. Information Technology (Logical) and Physical Security technologies
2. The integration of Physical and IT Security Systems
3. Integrated Security Management

Information Technology (Logical) and Physical Security Technologies

Physical security systems can be considered to be IT systems used for the purpose of physical security. A good example are Physical Access Control System (PACS). PACS controls the physical access to buildings and other physical facilities. It consists of a database management system connected to an electronic access device such as an Radio Frequency Identification (RFID) card reader or a biometric device to allow physical access (Forristal 2006).

Logical security technologies are used to protect the computer systems and the data assets contained in an organization, such as identity management, access control, and network security systems, These technologies do not have any interaction with the physical security systems.

The integration of IT and physical security systems

The integration of IT and physical security systems has one base element, the creation of a single sign-on token. The implementation of the single sign-on token establishes a consolidated repository of user credentials, giving organizations total control over the access of physical and logical assets (Forristal 2006; Imprivata 2006; Mehdizadeh 2003). The convergence model suggests that the single sign-on token will be embedded in an Identification Card, like the smart cards currently used for physical authentication. Currently, there is an initiative from the U.S. Government for a single sign-on card implementation. This initiative is the Personal Identification Verification (PIV) Card that resulted from the Homeland Security Presidential Directive-12 (HSPD-12) to enhance the identification process for all federal employees and contractors.

A converged security solution begins with a central control system in charge of consolidating the identities used by the all security applications and to function as a gateway (Imprivata 2006; Forristal 2006). Emerging gateway technologies are starting to bridge the gap between physical and logical systems by providing a bidirectional exchange of identity information and real-time security events (LaRoche 2006). The central system will contain the security policy, reports, events, and the repository of identities. As a result, organizations will be able to push a single security policy across the enterprise to control the access to physical and logical infrastructure (Forristal 2006; Imprivata 2006; LaRoche 2006; Ting, 2006). In addition, organizations will be able to manage the security reporting and security events notification process from a central location that interfaces with all the security systems across the enterprise.

Integrated Security Management

A common misconception about security convergence is that it can be accomplished by merging the physical security and information security operations (Forristal 2006; Mehdizadeh 2003). While integrating the management of both operations is required, merging them is not the solution. According to Steve Hunt, an analyst from Forrester Research, the most successful convergence projects allow the physical and IT security departments to retain their autonomy (Forristal 2006). This is because security management integration is a crucial element of the security convergence process and perhaps the most cumbersome. Integrated Security Management is the consolidation of the physical security and logical security management functions (Bernard 2006).

STANDARDS AND INITIATIVES

The integration of security applications is a major step in the convergence process. Yet, it depends on the ability of different applications communicating between each other in order to mitigate the security risks faced today. This is a complex task because of the many discrepancies that exist between the different systems. In addition, the lack of standards have prevented many organizations from fully exploring convergence and these organizations have decided instead to wait until vendors and system integrators work out the divergence that exists between these systems (Forristal 2006). However, presently there are a number of standards and initiatives working to close the gaps created by the lack of standardization. Some of the most noteworthy are the Physical Security Bridge to IT Security (PHYSBITS), Open Building Information Exchange (oBIX) and the Homeland Security Presidential Directive-12 (HSPD-12). Two of these standards, PHYSBITS and HSPD-12, are discussed below.

Physbits

The Physical Security Bridge to IT Security or PHYSBITS - developed by the Open Security Exchange (OSE) - is an open standard that enables the interoperability of security applications. PHYSBITS offers a framework and a data exchange protocol designed to facilitate the communication and interoperability of security applications from different vendors.

Some experts believe that earlier efforts to enable security integration such as PHYSBITS were slowed down by the lack of an open communication standard (Roberts, 2007). That was until the emergence of the eXtensible Markup Language (XML). Consequently, a data protocol for PHYSBITS has been under review for a few years and has been incorporated with XML to create what is known today as the Security Event Data Mark-up Language (SDML). This data exchange protocol is designed to create a normalized data structure utilizing the traffic generated by security alerts or events triggered by the different security systems. The normalization of the security events data is a crucial step towards convergence. The main goal of the process is to create a standard structure that can be shared by applications to relay information between each other while maintaining the integrity of the data that is currently included in these events. As a result, the OSE has defined a data scheme that includes who, what, when, where and state of a security event. These fundamental attributes carry ample information that a security system can use to react to a security event.

Homeland Security Presidential Directive-12 (HSPD-12)

On August 27, 2004 President George W. Bush issued the Homeland Security Presidential Directive-12 (HSPD-12). HSPD-12 proposes guidelines for the implementation of a Federal standard for a secure and reliable form of identification by which federal employees and contractors are granted access to facilities and information systems. Fundamentally, HSPD-12 called for a new Identification Card that would provide both physical and logical access to all federal facilities and systems (Forristal 2006). In response to the Presidential Directive, the National Institute of Standards and Technology (NIST) released the Federal Information Processing Standard 201 (FIPS 201). FIPS 201 lays out the technical specifications for a Personal Identity Verification system that establishes a secure and reliable identification of Federal employees and contractors as demanded by HSPD-12 (NIST 2006). The standard is structured in two parts. The first part lays the foundation for the security requirements and the controls of the new identification system including proof of identity, registration, and issuance of the card itself, as stipulated in HSPD-12. The second part provides the technical specifications to support the processes for the system described in the first part, but most importantly for the topic at hand, it describes how this system is going to interoperate among the different departments and agencies. This new ID card provides a single, common credential to be used for both physical and logical access across different facilities and buildings.

PRE-IMPLEMENTATION CHECKLIST

The integration of IT technologies and security systems with information makes security convergence more feasible. However, there are many differences between the physical and logical security systems that have made the convergence process extremely complex and costly (LaRoche 2006). For many organizations, the challenge of implementing security convergence begins well before the implementation of specific technologies or standards. Many prerequisite decisions, both technological and managerial, must be made and instituted prior to convergence implementation.

Project management provides a structured procedure for attacking IT-related problems (Turner 1993). The classical view of project management (Fayol, 1949) views projects in terms of five basic management functions: (1) planning the work to be done, (2) organizing the resources to do it, (3) implementation by assigning work to people, (4) controlling progresses to achieve the plan or replanning if necessary, and (5) leading the team. The *organizing resources* phase is needed to make pre-implementation decisions regarding technology, software, etc. This provides a plan of attack for the rest of the project with regards to resources utilized.

The following pre-implementation checklist is a listing of areas which need to be addressed by the organization when organizing resources for a security convergence project.

- *Database*
  Analyze the backend database layouts for each security area. Look for necessary fields for each area as well as data specific to each. Also, decide how to integrate the two systems with as little repeated data as possible.

- *Telecommunications*
  Examine your company's current network infrastructure. If it is necessary, you may need to install extra lines or setup wireless devices so the two systems will be able to interact using the same communications network. Also, conversion of physical security systems to IP-based protocols is necessary.

- *User Interaction*
  Evaluate user needs with regards to interaction with the system. Which users will need what type of interaction methods? Will new graphical user interfaces (GUIs) need to be developed. If necessary, interview workers who will be involved with the system to get feedback on these mechanisms.

- *Corporate Policy*
  Thoroughly layout the various policies which will dictate updates, changes, etc. to the system. Also layout a chain of command for who will be in charge of what pieces once the new system is installed.

- *System Security*
  While the converged system will provide for greater security through an integrated environment, the system also provides potential for greater security risks as all security is centrally housed and managed. Make decisions about the security of the system such as the mechanisms, both physical and logical, which will be instituted to protect the data and instruments from malicious insiders and outsiders as well as accidental employee error.

Included under each of the five primary areas above, three separate sub-decisions must be made regarding the area as it pertains to both the physical and logical security implementations.

a. The physical security sector
b. The logical security sector
c. The integration of the physical and logical security sector.

Table 1 provides a graphical representation of the security convergence pre-implementation checklist across the areas of convergence.

Table 1: Convergence pre-implementation checklist

Component	Infrastructure	
	Physical	Logical (IT)
Database	Add needed fields Remove repeated fields	
Telecommunications	Convert to IP-based	Install new lines Attach to Physical system
User Interaction	Create Management applications	Create Security personnel applications
Corporate Policy	Update corporate security policy	
System Security	Update/Install physical and logical security mechanisms to protect the new system itself	

Table 2 shows where this checklist appears in a classic project management scenario.

Table 2: Classical Project Management with the Security Convergence Pre-implementation checklist included

Project Management		
1	planning the work to be done	
2	organizing the resources to do it	
	a	Database
	b	Telecommunications
	c	User Interaction
	d	Corporate Policy
	e	System Security
3	implementing by assigning work to people	
4	controlling progress to achieve the plan or replan if necessary	
5	leading the team	

Due to this large combination of nested decisions, we believe that the above checklist is needed by those considering implementing security convergence during the *organizing resources* stage of project management to aid in decision-making. The checklist provides implementers with a concrete delineation of the exact resources which will need to be considered during the course of the project.

CONCLUSION

The concept of Security Convergence, as discussed in this paper, provides a viable solution for creating a more efficient and rigid security environment. Physical security operations, although having been around for many years, have gone through significant changes in the past few years. The fact that information technology has been rapidly incorporated into the physical security environment indicates the demand for more accurate and manageable systems. In addition, the sequence of security threats that information technology systems are constantly facing, plus the novelty of the logical security operations, are forcing a modification to the way that organizations are approaching security.

This paper provides an overview of the topic of Security Convergence and the standards currently incorporated. The paper also provides a pre-implementation checklist for those organizations who may wish to incorporate the technology in the future. This checklist is intended as a starting point in a corporate initiative towards security convergence.

REFERENCES

Bernard, R. "Convergence and the Security Industry," *Security Systems and Services(USBX Advisory Services)*, Retrieved on 28 January 2008 from http://www.usbx.com/industries/security/Advanced%20Convergence%20Themes%20in%20Security.pdf.

Booz Allen Hamilton. "Convergence of Enterprise Security Organizations," *The Alliance for Enterprise Security Risk Management*, November 2005, pp. 1-27.

Contos, B.T., Derodeff, C.,Crowell, W.P., Dunkel, D. *Physical and Logical Security Convergence: Powered By Enterprise Security Management*, Syngress, 2007.

Fayol, H., *General and Industrial Management*, Pitman, 1949.

Forristal, J. "PhysicaLogical," *Network Computing*, November 2006.

Hoffman, T. "Security Convergence," *Computer World Security*, February 2006, Retrieved on 28 January 2008 from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=108571

Imprivata. "Bridging the Great Divide - The Convergence of Physical and Logical Security," May 2007, Retrieved on 28 January 2008 from http://securitysa.com/regular.aspx?pklRegularId=3211.

Kinslow, J. "Physical and IT Security: The Case for Convergence," *Journal of Security Education* (2:1), 2006, pp. 75-91.

LaRoche, G. "Information and Physical Security: Can They Live Together?" *Information Systems Security*, December 2006.

Mehdizadeh, Y. "Convergence of Logical and Physical Security," *Information Security Reading Room (SANS Insitute*), October 2003, pp. 1-22.

NIST. "FIPS 201 - Personal Identity Verification of Federal Employees and Contractors," Federal Information Processing Standards Publication, March 2006, Retrieved on 28 January 2008 from http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

Roberts, P. "Security gets Physical," *Info World* January, 2007.

Ting, D. "Bridging Physical Access Systems and IT Networks," *TechNewsWorld*, November 2006.

Turner, J.R. *The Handbook of Project-Based Management*, McGraw-Hill, London, England, 1993.

Whitman, M.E. "Enemy at the gate: threats to information security," *Communications of the ACM* (46:8), August, 2003, pp. 91-95.