Continental Automated Buildings Association

Information Series

IS 2008-146

When Worlds Collide: The Convergence of Physical and Logical Security

CABA
www.caba.org

When Worlds Collide: The Convergence of Physical and Logical Security

Reprint Date: November 2008

Honeywell Novell.

When Worlds Collide

The Convergence of Physical and Logical Security

White Paper

www.honeywellintegrated.com

Table of Contents

Although traditionally separate entities, physical and logical security departments in the government sector are successfully joining forces to provide organizations with the maximum amount of protection. Is your organization ready to take advantage of convergence by integrating disparate security efforts?

Two Worlds, One Mission

All enterprises commission their physical and logical security professionals with the same mission – securing critical assets. Whether to ensure only authorized personnel can access a building or a network, both ends of the security spectrum are focusing their efforts on letting in the right people. Ultimately, these two departments work toward the same goal, but approach it from different perspectives.

With different approaches to security, why are physical and IT security professionals now working to integrate their systems? To answer this, let's consider the origins of security convergence. Traditionally, physical and IT security departments have been kept separate, but as risks continue to increase, federal regulations have made convergence a top priority for the federal sector. Now, as federal agencies achieve success with mitigating security risks, commercial organizations are beginning to mirror this convergence initiative.

Laying a Converged Foundation

Converging the efforts of physical and logical security departments allows an organization to significantly lessen security risks while also saving time and money. Once integrated, these two departments collaborate to ensure physical access to buildings is linked closely with logical access to computers and network resources. Similarly, actions to revoke an employee's physical access can be used to trigger automated network deprovisioning on the logical side – ensuring both departments are consistently on the same page when it comes to enterprise security.

To reap the full benefits of a converged security system, your enterprise must start with a solid identity management solution that is integrated with a physical access control platform, allowing you to closely tie physical and logical security initiatives together. The identity solution manages all user identities and protects information resources and business systems from unauthorized access, while the access control platform manages all physical access control, alarm monitoring and badging systems. With this integration, enterprises obtain an identity-enabled infrastructure to automate the management of roles and secure access to information and facilities.

Once this foundation is laid, automated user provisioning is critical to control user access across disparate systems while also gaining a holistic view of access occurrences. Convergence allows an organization to create a single unified security policy across the entire organization, removing the security silos of the past. Convergence also reduces cost and increases productivity by simplifying

the process of manually managing identity information across several systems. Now, user data can be automatically synchronized across multiple facilities and systems, allowing security personnel to maintain a single point of management for all users, update role changes and terminate user access. The end result is tighter security controls across all organizational systems.

Considering the benefits convergence provides, why isn't it being widely adopted? Like any business model shift, a main driver is necessary to get the ball rolling. As such, the catalyst for convergence started in the federal sector in the form of a regulation called HSPD-12.

HSPD-12: The Birth of Convergence

Convergence is not a topic that was common – or even considered – for enterprises as recently as five years ago. Following the tragic events of September 11, government agencies experienced a call to action to significantly increase security efforts. The perpetual threat of terrorist attacks, combined with increasing occurrences of identity theft and unauthorized access to federal buildings and information systems, drove President Bush to sign Homeland Security Presidential Directive – 12 (HSPD-12), a federal regulation mandating that all federal agencies implement a personal identification verification system. This act caused the federal government to embark on the largest convergence project in history.

With a deadline of October 2008, HSPD-12 has motivated government agencies to be proactive in converging physical and logical initiatives. This regulation will not only allow government agencies to greatly increase their security standing, but will also save significant amounts of time and money. Fundamentally, by having the same ultimate goal to protect assets, both the physical and logical security departments encounter overlap as they perform their respective jobs.

If It's Good Enough for Uncle Sam...

With all the buzz around HSPD-12, it may seem as though the convergence trend is solely geared towards the federal sector. However, as government agencies achieve success by converging security efforts, the trend is spreading to the commercial sector and gaining momentum in several high-security industries, such as healthcare and financial services. Forrester Research has 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.

From the commercial perspective, insider threats continue to plague organizations, as many don't effectively monitor what each employee can access in terms of the physical building and the network. By converging security initiatives, each employee is provisioned to only access authorized enterprise assets, eliminating the risk insiders (whether malicious or ignorant) can pose.

As the mobile workforce increases, remote workers inevitably bring new security issues to light. With identity management, organizations use roles and access rights to block remote users from inappropriate systems when outside the firewall. Securing remote access is also crucial when deprovisioning terminated employees. If an employee is denied building access on his last day of work but can still access the network remotely for days or even weeks later, there is a window for disaster. By controlling who can enter a specific room or computer application, the potential for damaging security breaches is decreased considerably.

Convergence is also important as organizations enter into mergers and acquisitions, or experience increased personnel growth. These transitions can be quite an undertaking, as thousands of users need to be provisioned to access the correct resources in a timely manner. Without this integration, enterprises have to manually provision and deprovision user access to all enterprise assets – costing organizations a significant amount of time and money, and leaving gaps in enterprise security.

It is the nature of business to constantly evolve and grow in complexity. Each day, organizations are faced with new challenges and opportunities allowing them to advance their operations. In order to effectively leverage each opportunity, organizations must ensure their security practices are rock solid. Converging enterprise security initiatives is the necessary step to prepare your organization for continued growth and success.

So You're Making the Move to Converge...Now What?
The case has been made for making the move to converge physical and logical security initiatives, but where exactly does one begin? The following list suggests tips and tricks to consult before integrating these two efforts.

- **Do** ensure the solution includes an identity management component that is integrated into an access control platform. With this foundation, you can be confident that access to both physical and logical assets is linked back to the user identity – confirming only authorized users gain access.

- **Don't** strive to merge the two departments entirely. Forcing these disciplines into one security bucket will only cause chaos. Each department should maintain its role in the organization; however, structured collaboration is the key to success.

- **Do** make automatic provisioning/deprovisioning a priority. This feature is critical, as it relieves organizations of the tedious, manual task of provisioning – saving precious time and money. It also increases employee productivity, protects from the insider threat and immediately denies access to all former employees.

- **Don't** let fear or unfamiliarity hold you back. Research various solutions, best practices and approaches to determine what specific technology is the best fit for your organization. Convergence is the future of security, so it is imperative to understand the topic and how it can help your organization succeed.

A Worldwide Call to Action

Considering the various facets of security threats (terrorism, identity theft, data breaches, insider threats, etc.) one side of the security spectrum simply cannot protect an organization to its greatest potential. Integration provides a holistic view of access occurrences across the entire organization – keeping a vigilant eye to ensure only the right people gain access to the enterprise, from the front door to the keyboard. In addition to enhanced security, automatic provisioning/deprovisioning allows organizations to save significant amounts of time and money, as manual processes waste valuable resources.

An initiative that began with our nation's most secure networks and facilities, convergence is inevitably the future for enterprise security and continues to gain traction in the commercial sector. As businesses grow in size and complexity, security measures feel the brunt of these growing pains all too often. With a converged security model, efforts are combined to ensure organizations achieve a comprehensive view of *all* access occurrences, providing the highest level of security while saving valuable time and money.

Going Forward

Over the coming months, Honeywell will introduce several technologies that will allow your organization to take advantage of the convergence between IT and physical security. Given all of the benefits of a converged system—productivity from common protocols, increased security of physical assets and data, and improved ROI on IT and security infrastructure investments—Honeywell is positioned to be your partner of choice for converged solutions. For more information, visit www.honeywellintegrated.com.

About the Authors

Ivan Hurtt is the primary product marketing manager for Novell's Identity & Access Management products. Prior to this role, Mr. Hurtt served as the product manager for Novell's flagship directory services product, Novell eDirectory. A member of the United States National Guard, Mr. Hurtt served in Afghanistan.

Peter Fehl has been with Honeywell for the last four years and has held several positions within the $10B Automation & Control Solutions business. He currently works in the Honeywell Security business leading marketing initiatives and driving business development and strategic direction for the Integrated Security segment. Prior to this role, Mr. Fehl led the mergers and acquisitions group for the Honeywell Process Solutions business.