



**Physical/IT Security Convergence:
*What It Means, Why It's Needed, and How to Get There***

OSE
1444 I Street NW, Suite 700
Washington, DC 20005 USA
Phone: 202.712.9058
Fax: 202.216.9646

Introduction

Today's corporate security infrastructure is a patchwork. Most organizations maintain multiple, separate physical and IT security systems with no integration among them. This situation has become a growing liability as security concerns and the need to address privacy and regulatory compliance issues grow. At the same time, it prevents organizations from realizing an array of cost, control, and responsiveness benefits.

The Open Security Exchange (OSE) was formed to address these concerns and enable these benefits. 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. Its goal is to help improve enterprise security through the collaborative development of reusable models, definitions, vendor-neutral interoperability specifications and best practice guidelines that accelerate the convergence of security systems.

This white paper is part of that effort. It discusses what convergence means for businesses, the business drivers for convergence, and the OSE's Convergence RoadmapSM to help organizations plan for and achieve convergence.

The Coming of Physical/IT Security Convergence

Today, virtually all organizations with physical and IT assets protect those assets in a variety of ways. There are alarm systems to protect facilities and their contents from unlawful entry. There are firewalls to stop intrusion into corporate networks. Corporate assets may also be safeguarded by the use of employee ID badges, software application passwords, and a growing number of technologies, from magnetic cards and readers to biometric finger scans. The scope of security systems spans physical access, logical access, video surveillance and storage, identity management, and more.

While all of these security technologies share a common purpose, those that protect physical assets and those that protect IT assets have virtually nothing else in common. They have always existed in parallel, evolving separately and residing under the control of separate organizations. This has resulted in a lack of integration and interoperability between physical and IT security systems.

With today's heightened security concerns, this lack of integration is no longer simply an inconvenience. It increases security risks by preventing technologies from working in concert with one another. It limits corporations' efforts to establish centralized control of security and develop integrated risk management strategies. It prevents coordinated responses to security breaches by physical and IT security systems. With no integration between physical and IT security systems, organizations cannot pursue cost synergies, fully address privacy issues, or ensure compliance with a growing number of government and industry regulations.

The solutions to these problems will come from the convergence of physical and IT security technologies.

What is Convergence?

The OSE defines convergence as the migration of physical and IT security towards common objectives, processes and architectures. This migration includes:

- Objectives:
 - Cost reduction/Revenue enhancement/Regulatory compliance
 - Improve asset/personnel protection
 - Improve operational efficiency of physical/IT security staff

- **Processes:**
Collaborative planning between physical/IT staff on security strategy
Identify/eliminate security gaps
Best practices and policies for converged security
- **Architecture:**
Strategic, tactical and operational security modeling
Interoperability standards and policies for physical and IT systems
Combined credentials for physical and logical security

Physical/IT security convergence will enable vendor-neutral interoperability among diverse security components to support overall enterprise risk management needs. As physical and IT security merge, networked computer technology and associated applications will provide enterprises with increased operational efficiencies and intelligent security.

The Business Case for Convergence

Every organization has its own security needs and concerns, as well as its own business goals. One way to begin identifying and prioritizing your organization's key convergence goals is to consider common business drivers and their relationship to security convergence.

Risk management is a common theme among security-related business drivers. Therefore, risk assessment techniques are very useful in identifying and prioritizing an organization's security agenda. This enables companies to target scarce resources at the most likely and potentially damaging threats.

Among the most common business drivers are the following:

Compliance

The requirement for certain mandatory actions and outcomes is common to IT and physical security, and is therefore a candidate for a converged approach. This driver involves staying abreast 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. All of this must be achieved at the minimum possible cost without making a negative impact on compliance performance.

Besides these enterprise-wide compliance needs, certain operations, departments, or divisions within a facility may have their own, more stringent compliance requirements. An interpretation of a compliance/regulatory requirement should first consider the group with the highest level of risk mitigation and use that standard as a base line for the remaining groups. For example, in the financial services industry, it is not unusual for a retail bank to share a facility with a mortgage origination operation and a securities brokerage division. By addressing the most stringent security requirements among these groups, organizations can ensure better security for all.

Compliance factors include:

- **Regulations.** These are government-promulgated mandates, such as Sarbanes-Oxley, employment and privacy laws, HSPD-12, and the Health Insurance Portability and Accountability Act (HIPAA).
- **Policy and procedure.** These are the fundamental, internal requirements, typically related to and driven by Human Resources.
- **Workforce security awareness.** It is essential that all members of the workforce understand that security is everyone's responsibility, not just the responsibility of the security professionals.

Asset/Personnel Protection

Both physical and IT security systems are designed to protecting an organization's revenue-producing assets -- including people, equipment, products, tools, and information. Organizations need to understand which assets need to be protected at what level of assurance, then develop and operate a mechanism to grant access to those assets. With a mechanism in place, they need to be able to monitor and analyze access (both historical and real-time), and respond to inappropriate access.

Typical asset and personnel protection factors include:

- **Authentication.** Organizations need to determine whether a person, computer, or web site is indeed who or what they claim to be, and find a convenient and secure means to persist such determination (e.g., badges, passwords, etc.). The level of trust placed in establishing and persisting identity should match the value of the assets being protected.
- **Authorization.** This is the process of granting appropriate access to assets based on identity and/or other attributes; that is "letting the good guys in, keeping the bad guys out." Organizations need to make sure that the needed access to assets is granted in a timely manner, that access is properly monitored, and that they can respond effectively to inappropriate access attempts.
- **Integrity (non-repudiation).** This means having the ability to trust -- and prove the authenticity and change history of -- tangible and information assets. Examples include being able to prove a signature on a wire funds transfer, or that a security videotape has not been altered.
- **Brand equity/goodwill.** This is a special class of asset protection that often merits special attention from both IT and physical security. It strives to assure that the public's trust in the organization and its products and services is not damaged through lapses in security.
- **Personnel protection and life safety.** Involves traditional executive protection, insuring a crime and offense-free workplace, and the ability to account for and assist personnel in emergencies.

Business-Building

Most organizations treat both physical and IT security as a necessary cost of doing business, not a revenue or profit enhancer. It is difficult to quantify the business-building benefits derived from having employees who feel safe in their work environment, even though everyone would intuitively agree that the benefits are there. Nevertheless, both IT and physical security practitioners frequently look for ways to recast and enhance their mission statement to include business-building goals. Often this means transforming security from a cautionary hurdle in business ventures to a confidence-inspiring "ready, go" capability. The resulting acceleration in decision-making and other management processes can help the organization capture opportunities it might otherwise lose. By combining best-of-breed practices and solutions, physical and IT security professionals can achieve this transformation.

Key business-building security factors include:

- **New business models.** Security measures must be able to keep an organization's assets secure while participating in business models involving outsourcing (to level "n"), contract manufacturing, partnerships, or other joint ventures.
- **Mergers and acquisitions.** Organizations need to be prepared to quickly assimilate another organization's security structure.
- **Business continuity.** By sharing best practices across IT and physical security, organizations can ensure that normal operations (and thus, revenue streams) can be restored more quickly after a loss event. These measures may also decrease the likelihood of the loss itself.

Cost Control/Productivity

Both IT and physical security involve investing to lower risk. One can think of an “efficient frontier” curve on a graph of security investment versus risk, with each point on the curve representing the lowest risk for a given investment and/or the lowest cost for a given level of risk. Not only do IT and physical security professionals strive to operate on this most efficient frontier, they also strive to bodily move this curve by lowering costs for all levels of risk. Once again, combining best practices and solutions from both physical and IT security can help make this happen.

Cost control and productivity factors include:

- **Convenience and usability.** When day-to-day secure behavior is effortless, it increases user productivity. Examples include making it easy to securely obtain or reset credentials, single sign-on, ease of requesting and granting access to assets (doors, servers, etc.), and the use of badges for canteen operations. The security goal is to allow a worker to go to from the street to a desk and be logged on to a company’s network with as little efforts as possible without compromising security.
- **Process reengineering.** This refers to efforts to drive efficiency into all security-related processes, such as incident response, security monitoring, credentialing, policy-making and exception-granting, governance, vulnerability testing, security auditing, and reception.
- **Workflow automation.** By applying automation to the processes listed above, an organization may be able to shorten cycle time, eliminate human errors, and reduce effort.
- **Workforce optimization.** When an organization realizes greater efficiencies in security, it may reduce resource requirements or thus enabling the reassignment of personnel to more strategic, business-building activities.

Physical/IT Convergence Roadmap

The OSE has established a Convergence Council, a group of senior security and IT executives from blue chip organizations, the purpose of which is to create reusable models, definitions, and tools to enable organizations to advance convergence.

The Council’s current key project is the Convergence Roadmap, a multi-faceted tool that will provide illustrative, diagnostic, and theoretical aids to enable convergence. The Convergence Roadmap will include taxonomy and definitions associated with convergence, and will be agnostic to an organization’s current convergence status.

The Convergence Council will create separate Roadmaps for physical and IT security. Each one will provide a structured guide to understanding and advancing convergence, beginning with an ideal end-state and offering several points of entry or interface (“on-ramps”), as well as milestones to assist organizations in their journey to convergence. Organizations will be able to browse the Roadmap via a web-enabled representation with drill-down capabilities into areas of specific interest. By interacting with diagnostic tools, each organization will be able to customize the Roadmap to its needs and goals.

When completed, the Roadmap will help you determine:

- What convergence means to your organization;
- How it can add value;
- How to know when you are ready to converge;
- How you can leverage your current investments; and
- How the old and new solutions/products fit together.

This invaluable tool is currently in development with an initial release planned for Spring/Summer of 2007. Watch for a flash demo of the Roadmap to Convergence at www.opensecurityexchange.org.

Become part of the convergence movement

The convergence of physical and IT security is already happening. According to a November 2006 a Lehman Brothers report states that “growth will come in systems that identify and authenticate a potential ‘entrant’, and then tie those credentials into the company’s IT infrastructure.” That same report charts the Convergence Market at \$150M and growing at 82% CAGR.

For more information on the OSE and details on becoming a member, please visit www.opensecurityexchange.org or call (202) 712-9058.

As a member of the OSE, Imprivata has worked collaboratively with other members to help establish guidelines, models, specifications and definitions. Imprivata is a proponent of the advancement of Convergence and an advocate of the OSE’s methodologies.

Imprivata® OneSign™ Physical/Logical integrates network and building access systems to provide a single consolidated user identity allowing organizations to implement one comprehensive, converged policy for allowing or denying network access based on a user’s physical location, role, and/or employee status. For information on OneSign P/L please visit www.imprivata.com or call 1-877-OneSign.

OSE
1444 I Street NW, Suite 700
Washington, DC 20005 USA
Phone: 202.712.9058
Fax: 202.216.9646



www.opensecurityexchange.org