A bnp media Publication

February 2007

SDM

New Directions for Secur[illegible]egration

Convergence Here & How

Wayne Smith is leading the charge at Tech Systems to embrace the change that IT and the business community is demanding today: physical and logical security convergence.

sdmmag.com

CONVERGENCE HERE

Security integrators are finding that convergence of building security and computer security is something customers are demanding – and integrators need to ready themselves for this market.

By Laura Stepanek, Editor

PHOTO FOR SDM BY BILLY BROWN

Every weekday morning I fumble for my two access cards. One unlocks the door to my office building, and the other unlocks the door to the suite where *SDM* is published.

At my workstation I use one password to log into the network, and another to start up my e-mail program. It's a routine I am accustomed to, but security professionals explain there is a more efficient — and principally — more secure way to do business.

It involves the convergence of physical security with logical security. "Convergence" is popular talk among industry professionals, but what does all the talk boil down to?

It's important to first distinguish between security convergence and the convergence of IT and physical security, says Steve Hunt, CPP CISSP, founder of 4A International, a security convergence research firm in Chicago.

"It might sound like word play, but the highest level of convergence is merely the use of IT (computers, software and networking) to do physical security better. That creates a new breed of physical security products, like IP cameras, DVRs, NVRs, IP-based access control, and managed services or hosted services," Hunt says.

The next tier of convergence, Hunt reveals, is the convergence of physical security with IT.

"The merger with IT security…involves IT security professionals and creates the idea of riding security policies across two very distinct groups in an organization. That brings in a human dynamic, corporate policy and touches on industry regulations like Sarbanes-Oxley Section 404, which says among other things, that all computerized financial transactions must be properly audited.

"That sounds simple, but if I'm an unauthorized user and I touch a computer that's logged into a financial application, I performed a financial transaction, so that's a violation of Sarbanes-Oxley. It's a physical security problem because I was in that room, but it's a computer problem," Hunt thinks.

& HOW

Through partnerships between traditional security manufacturers, such as ASSA ABLOY (parent of HID Corp.) and IT companies such as Cisco Systems, for example, solutions that address potential compliance problems are quickly becoming a reality. For example, these two companies announced last September their collaboration to bring a physical and logical access package to the market.

What this means is a single system that protects physical facilities, such as doors, and logical facilities, such as corporate computer networks.

"Both doors and networks provide access to resources and assets, whether they are material, intellectual or financial," Cisco Systems stated in an announcement about the collaboration with ASSA ABLOY. "Historically, physical and network security systems have been independent and isolated from each other. The theft of money or intellectual property can be carried out physically or electronically," the company explained.

The solution is called Hi-O, for Highly Intelligent Operation lock technology. It uses ASSA ABLOY standards-based Hi-O enabled products including electronic access control and video surveillance, with Cisco System's IP network solutions built on its Intelligent Converged Environment platform.

Hi-O products allow for physical security products to communicate with each other, as well as the IT network. For example, if an employee badges into the building via an access control badge reader, that employee then would be allowed to log into his or her computer. If the employee doesn't badge in, he or she is thought of as not in the building and therefore, would not be able to sign on to the network. Such an arrangement "creates best practices that can help address compliance verification requirements," Cisco explains.

In the middle — between the vendors like ASSA ABLOY and Cisco, and the end-users in need of tools to help them deal with compliance — are systems integrators who are gearing up to be specialists.

PHOTO FOR SDM BY BILLY BROWN

Tech Systems' Nytee Nobles uses her smart card to log into the company's computer network.

Off to a running start is Tech Systems Inc., Duluth, Ga., the 28th largest security systems integrator in the United States (*SDM*'s Top Systems Integrators report, July 2006).

Last November, Tech Systems hired Wayne Smith, CISSP, as vice president of its Network Services Group. Smith had been the director of information security for a large global payment processor.

"My role is to bridge the gap between the physical security personnel and the IT departments. By doing so, both our customers and Tech Systems will benefit," Smith pronounces.

"The physical security market has been moving slowly toward convergence for some time. Meanwhile, the IT and business community is demanding it today. Tech Systems has embraced this change," Smith says.

Smith is familiar enough with the security industry to understand that some explanation may be necessary here: How can physical security and logical, or IT, security be converged?

"Traditionally, the physical security system has been maintained separately," Smith explains. "But now we're providing more opportunities for integration with things like single sign-on technology, smart card integration for physical and logical access, IP-based video systems and other network-centric security devices," Smith conveys.

Some of the vendors serving up such possibilities are traditional physical security vendors such as Stockholm, Sweden-based ASSA ABLOY and Bioscrypt, Markham, Ontario. Others are new to the security industry, such as Imprivata, Lexington,

WHERE TO LEARN MORE ABOUT CONVERGENCE TECHNOLOGY, TRENDS

ASSA ABLOY
www.assaabloy.com
46 506 485 10
(in Sweden)

Bioscrypt
www.bioscrypt.com
(905) 940-7750

Cisco Systems
www.cisco.com
(800) 553-6387

4A International
securitydreamer.com

Imprivata
www.imprivata.com
(781) 674-2700

Mass., and Cisco Systems, San Jose, Calif., which have strong roots in the IT industry and now are extending their reach into physical security.

Imprivata's initial business had been providing secure user authentication to a network, reports Geoff Hogan, senior vice president, business development and product management, "and once the user is on the network, providing them single sign-on to manage access to all the enterprise applications they use in their daily course of business."

PHOTO FOR SDM BY BILLY BROWN

Tua Chai, director of technical services at Tech Systems, configures a user for smart card authentication on the network.

Single sign-on is a system for managing passwords for secure access to a network and user multiple applications on that network.

"Some of our customers — but a lot of prospects — said 'we really like your OneSign solution for single sign-on, but we have these building access cards that we've already purchased, and given out to our employees. Could you use this card as a form of authentication to the network?' And we said, 'that's a pretty good idea.'"

Hogan clarifies that a building access control system is a self-contained system with its own database of user information stored in it. A corporate network contains user identities typically stored in something like an active directory, which is totally separate from an access control database.

At the 2006 ASIS conference, the company announced its convergence product called OneSign Physical/Logical, a new module of its OneSign Authentication and Access Management platform. It allows organizations to grant or refuse network access based on a user's physical location, organizational role, and/or employee status. "It directly integrates with the Software House, Lenel and S2 Security access control systems," Hogan announces.

Bioscrypt Inc. enables the convergence of physical and logical access control with its Door to Desktop solutions, which the company believes simplify the task of implementing secure access to facilities, equipment and IT networks.

"The solution we're bringing to market through our partners is one of convergence theory. It's important to understand that to enable this convergence, there are no requirements to upgrade the infrastructure that an organization might have in place," says Matthew Bogart, Bioscrypt's director of corporate development.

"If an organization has a physical access control infrastructure in place (such as an HID reader, for example), they don't have to acquire new technology for physical access control to leverage a solution using Bioscrypt technology. They can have a card manage both the physical and logical access control, and use our software platform to enable the convergence," he adds.

Bioscrypt's solution comes to market through its partners, such as Lenel in this industry and Hewlett Packard and others in the IT industry. Many people associate Bioscrypt with biometric technology, and for good reason. The company specializes in biometric readers for both building access control and multi-factor authentication for PCs. However, its converged system does not require biometric access control, and can be used with any existing access control infrastructure.

"You're really creating a single identity for each employee and it's really a matter of using that identity for access — whether that identity is associated with a card at the door and a password at the computer, it's one person," Bogart acknowledges.

BEYOND THEIR ELEMENT

Why would traditional security companies want or need to get involved in IT security? What's prompting this dynamic change in the market?

"The IT people, chief security officers, and business leaders are all looking at ways that they can improve the bottom line and at the same time comply with the ever increasing internal and external regulatory requirements," Tech Systems' Smith acknowledges. "The converged market allows companies to maximize efficiencies, decrease response time, and streamline their back office support functions like security and investigations.

"We're not trying to get out of our element," Smith explains. "We are providing services that our customers are demanding. We can only do this by having the expertise and technical knowledge that these complicated systems require." ■