

Converging Security: Bringing two worlds together

By David Ting

This article will take a look at what convergence is and delve into a couple of the biggest, but often unexpected, issues that can arise once convergence has been given the green light.

Over the past few years, the idea of security convergence – integrating an organization’s building (physical) and IT (logical) access systems – quickly became one of the biggest future trends in the security industry. In articles, studies, and reports, convergence between the two disparate security systems was always described as something that would make security better for everyone involved – the IT staff, building security, executives, and those employees coming in and out of the office each day. In fact, Forrester Research 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 2008.¹ Practically everyone agreed about its importance and that it just made too much sense *not to happen*. The only question was when the idea would become reality.

Now that lower costs and better technologies have enabled organizations to implement security convergence solutions, it is easy to understand the basic benefits: stronger organization-wide security and easier, more efficient management.

However, as implementations have begun in several different industries, questions have started to arise about what type of convergence is best for an organization, how exactly this convergence will happen, and especially how it will affect company operations. Will security convergence force employees to change their daily routines and learn entirely new ways of working, thereby lessening productivity before it can be improved? Can security convergence be used by organizations as a way to finally enforce policies that have been previously unenforceable?

This article will take a look at what convergence is and delve into a couple of the biggest, but often unexpected, issues that can arise once convergence has been given the green light.

Making two into one

The word *security* always brings to mind the same things: safety and protection from danger. For years security was something in the background of an organization – the locks on the doors, the anti-virus software IT automatically updated. However, in this day and age, with identity thefts, insider threats, corporate espionage, and increased regulatory compliance worries, security is front and center. What used to be kept separate and under the control of different divisions, is now coming together and being jointly managed.

The term *security convergence* refers to the process of bringing together systems and data from the two historically separate security functions within an organization: building/physical security and IT/logical security.

Security convergence can take many forms, from traditional devices such as the television cameras monitoring the grounds being managed on the IT network, to more innovative ones such as integrating building access and IT access systems so that multiple identities in the two systems match up. The common thread is that security is approached as an overall, organization-wide problem requiring an integrated policy and approach in order to ensure all company employees and information assets are protected.

A link between an organization’s physical and IT security systems can take place on several different levels.

Simple collaboration

For some organizations, convergence can start with very low-level collaboration efforts: things as simple as the night watchmen making sure appropriate systems and desktops are shut down; to both groups teaming up to stop a fast-moving virus; or even cross-referencing video and images with known information about an individual or a vehicle, as has been happening for years at casinos. By working together as much as

¹ “Trends 2005: Security Convergence Gets Real,” Forrester Research, January 11, 2005.

possible, these two areas may come across other commonalities where convergence makes sense – and saves the company money. One of the easiest examples of basic collaboration is when employees are terminated, escorted out of the building, and removed from the IT systems on the same day. But as organizations soon find out, timing these two activities as close together as possible is of ever-growing importance.

Card-level convergence

The first potential link is where the organization sets up employees with smart cards that grant building/office access and then add the requirement that these same cards be used for entry to the IT assets as well. This means that one log-in credential can be used across both systems, naturally improving security across the organization but also reducing the cost of rolling out strong authentication should future plans or compliance needs call for that. This level of convergence can also reduce the number of credentials that a user has to remember or carry around with him, easing the burden on employees having continuous log-ins, multiple passwords, and pockets full of cards or devices.

However, this basic type of convergence at the card level does not actively link the physical and IT systems together: they remain in silos, collecting information and providing access, but not sharing that information or working together. This can become a huge security issue. For example, if an employee's physical access card is taken away upon termination and there is a delay in IT system access termination, the ex-employ or temporary contractor may still be able to gain access to Web-based applications and steal information or cause havoc.

System-level convergence

The second – and more secure – way of implementing convergence involves connecting the IT security and physical access system to share data and interact with each other. This approach better supports one organization-wide security policy for both physical and IT. In addition, this approach allows organizations to quickly and easily audit and report on employee activity across both the physical and IT systems, and to prove compliance with any relevant industry legislation such as PCI DSS or protection of citizen data.

Lastly, like card-level convergence, this approach can also cut the number of credentials that a user has to carry, helping employees to be more efficient and preventing them from being locked out of applications. Perhaps even more important is the fact that existing facility access cards can be used without having to re-issue new smart cards.

By having one single policy in place within an organization, policy violations such as tailgating, where a user forgets to log him or herself into the physical access system and instead enters behind a colleague, can be prevented. When physical and IT security is left unlinked and tailgating is allowed, security holes are exposed. A former employee could tailgate into the building and gain unauthorized access to critical or sensitive

customer and/or company information. Without badging in, the organization is also prevented from knowing who is in the building that day – something critical in emergency situations. With system-level convergence, when an employee that tailgated in tried to log onto the IT system, the system could query the building access database to check that user is a valid and current employee; if not, then the user can be denied access.

This level of convergence makes it even harder for someone without proper credentials to steal information, especially if he was a disgruntled terminated employee. Conversely, it also makes it much easier to activate and give the new approvals to a new hire.

Making convergence work

Converging security means that there is, theoretically, now only one single point of security management within the organization. However, in most organizations, this is not the case, and it may take some work and re-organization to get there. As a matter of fact, Forrester Research said in its 2007 convergence report that “Convergence is not about the unification of security into one environment, but about collaboration between environments. Both the IT security and physical security environments must be prepared and motivated for convergence to happen.”²

The biggest issues that executives grapple with when deciding to integrate physical and IT security are around company operations. Will employees need to change how they work; should they be made to change how they work; and how to get physical and IT staff to work together as one?

Employee adoption

It is up to each organization to decide exactly how to handle employee adoption of convergence. The very idea behind converged security is to add protections without adding more work for employees. At most, it will require some employees to remember to badge in each day and log in and out of the IT network each day – activities they should be used to. For the most part, it represents a way to increase security and lessen the burden for employees, as they have less cards/readers to carry and fewer passwords to remember.

Some organizations may want to go slower and ease into situations where employees cannot access the IT network or applications if they did not badge in that morning. An example might be to secure access to servers in the data center so they cannot be logged in without badging into the room. For some, especially those in the financial services or health care industries, it becomes an immediate requirement, as the converged security system is a protection for critical customer or company data, and a way to prove compliance with the latest regulations such as strong authentication at the point of trade in the financial industry; or in the health care industry, the

2 “Trends 2007: Physical And Logical Security Convergence,” Forrester Research, August 17, 2007.

proof of identity to dispense medication regulations. In those industries, there is no room for a slow roll-out.

Merging staffs

While a converged approach makes creating and enforcing security policy easier, it also may require changes in how the physical and IT security teams manage themselves. Traditionally, these have been separate parts of the organization – the staff at the security desk watching who comes in or out would only interact with IT when they needed assistance from the help desk and vice versa – but they now need to learn to share information and support each other for the common good.

Enabling better overall security by the convergence of the systems will require greater levels of co-operation between the two teams, as well as a wider understanding of mutual responsibilities. The first step is for the leaders of each side to show the importance of tight collaboration. No longer can one side shut the other out to handle certain problems or events.

Organizations should take the time when developing and implementing the system to make sure the needs of both groups are met and that the leaders of both the physical and IT side are involved every step of the way. IT security departments, for example, are only starting to deal with issues of insider threat and forensic investigations; something their physical security counterparts have far more experience with. Training and re-training both departments is another important aspect of this process so everyone starts at the same point.

This will lead to better understanding of each other's responsibilities – and a stronger sense of ownership of the converged system – giving both areas something to build off of for the future. If handled correctly, this change can make both physical and IT security professionals more effective in their respective roles.

The logical place for organizations to begin the merging of these disciplines is at the data center. With locks or readers on the doors and permissions needed to access information, it perfectly symbolizes the reasons behind convergence: to better protect access and simplify the process, pushing security

back to the behind-the-scenes safety and protection factor it always was.

Limiting risk is worth the risk

Security convergence does indeed add some extra complexities to the organization in the short-term, no matter how deep your convergence efforts go. However, no other initiative can reduce the security risks to your organization, your people and your data so easily while reducing overall costs for the organization.

Already, in the past three to four years this idea has grown from one that employees in IT and building security hated and thought would never be feasible to one that the industry has accepted as the strongest way to limit security risks, whether operating a 60-story office building with heavy daily traffic or a 100-person company with significant customer data or intellectual property to protect. There will still be hurdles to cross, opinions to change, and employees to re-train, but as organizations move in this direction, they will discover that over the long-term, the benefits truly outweigh any initial hurdles.

About The Author

David Ting is the CTO and founder of identity and access management company Imprivata. Named one of InfoWorld's Top 25 CTOs of 2006, David has more than 20 years of experience in developing advanced imaging software and systems for high security, high-availability systems. Prior to founding Imprivata he developed biometric applications for government programs and Web-based applications for secure document exchange. He was also a member of the scientific staff at the BNR/INRS Labs in Montreal, a collaborative research institution jointly operated by Bell-Northern Research and University of Quebec. He holds eight patents, has several patents pending and is a regular blogger at: <http://blog.imprivata.com> and can be reached at dting@imprivata.com.

