



Two Person Job: Integrating Beyond Security

by Ray Bernard, PSP

Return on Investment

One of the largest potential sources of return on investment for security systems comes from the integration of security with other systems. Integrating with Human Resources (HR) systems with access control for Time and Attendance was one of the earliest types of integration. That was followed by the ability to utilize an external database as the source of cardholder information. That allowed, for example, HR to assign parking privileges in its own system, with the parking access control system immediately implementing the privilege assignments (or cancellations).

The larger the enterprise is the more economies of scale can increase the financial benefits of integration. In 2004 Tatum Partners (www.tatumpartners.com) estimated that the payback from implementing common user provisioning (for enrollment and assignment of initial access privileges for both physical and information systems) was 18 months or less. That means that every year and a half the cost of implementing the system will be returned to the company over and over again. For a growing company, the return would actually increase as time goes on.

Other reports of significant benefits have many corporations eyeing such integration projects. In his Forrester Research, Inc.'s report titled, "Trends 2005: Security Convergence Gets Real"¹, security analyst noted Steve Hunt states, "In 2005, companies in Europe and North America will increase spending nearly threefold on projects that combine traditional physical security controls with IT security. That is, locks, cameras, entry systems, and even guard desks will be upgraded to work with the same computing systems that control computer and network sign-on, identity management, and security incident management."

That's integration far greater than what most security integrators have experience with.

If convergence was moving at a slow pace, that probably would not be a significant issue. But things are not moving slowly according to Forrester. The report states: "The market, currently described as the convergence of physical and logical security, is beginning to take off. Forrester expects private-sector spending to top \$300 million in 2005 ... Total spending on convergence projects in the public and private sectors in North America and Europe will exceed \$1.1 billion in 2005."

Some public sources estimate the project spending to be much higher than the Forrester estimates, due to projections related to government agencies and port authorities. Forrester doesn't think so, and the report's explanation hints at another significant aspect of today's integration projects: "Forrester does not expect actual spending to exceed this forecast because of political factors and the complexity of the proposed projects."

¹ Download from the Open Security Exchange at <http://www.opensecurityexchange.org/resources.html>.

The Complexity Factor

Today's convergence integration projects are very different from those of the past (even three years ago) in many ways. System complexity is just one of the factors:

- Today's integrated security systems are themselves increasingly complex, even without integration to business systems and IT security systems.
- New security technology is constantly being introduced to end users via industry shows, media articles and direct promotion.
- Information technology is a much bigger aspect of today's security systems.
- IT standards play a big role in security systems networking and integration requirements
- The IT landscape itself is evolving; this means that integrators now need continuous education on the IT aspects of integration.
- There is no "one place" that end users or integrators can go to get educated on the convergence integration aspects.
- The pace of change creates information overload for both end users and integrators.
- There seems to be no way to leverage the sunk costs of legacy systems, many of which are still at the beginning of their operational life.
- Where technology alone drives the convergence, projects become late or stall completely, while people cope with fitting the enterprise to the project systems.

All of these factors contribute to the complexity of projects. In fact, the apparent complexity that surrounds convergence keeps some projects from getting started at all.

Getting a Handle on Convergence Integration

It is common to start a convergence project's vision with a technology focus, which establishes a bottom-up orientation for the project. If the focus doesn't expand to match the technology up to security risk management objectives, strategies, policies and procedures, then the organization will have to somehow retrofit itself onto the technology. This one way that the valuable features of advanced security systems can end up unused. This results in lower return on investment and a less effective security system as deployed.

When integrators concern themselves with getting a handle on convergence, they usually think in terms of technology. That's natural—there is a lot of technology to get caught up in. The most successful convergence integrators know the real secret: *helping the customer to get a handle on convergence*. This is the most important factor regardless of the size of the integrator, the size of the customer or the size of the project.

Customer Collaboration is Key

The best projects start with the customer's own vision of what he or she wants to accomplish. This is not an equipment list or system specification. It's the vision of how the organization will go about addressing particular security needs, and how technology could or should be used to support that effort. Often new technology fits one or more long-standing security need that can now be addressed. Sometimes the excitement or relief at finding such technology can cut short the development of a full project vision, which includes mundane details like who will

have what responsibilities, and how these responsibilities will be executed, supervised and audited. Often security systems can support those processes and procedures, but without in-depth integrator/customer collaboration such system capabilities may not get utilized.

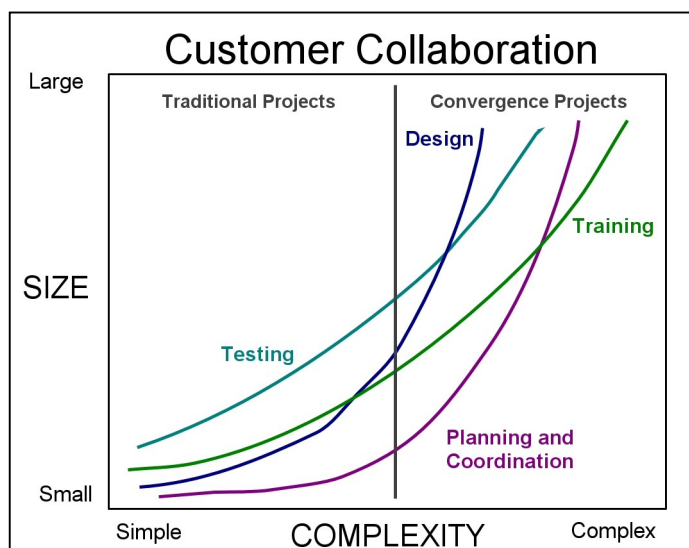
Collaboration Requirements

Today's systems have much greater capabilities and much broader scopes than those of recent years. For the near future, capabilities and scopes of convergence projects will continue to grow significantly. This means that the need to collaborate with the customer for design, commissioning and testing, as well as project planning and coordination, is much higher than ever before.

Figure 1 shows a very simplified concept of how size and complexity affect the customer collaboration requirements of security projects. There are many other elements that also affect the nature of the collaboration required:

- degree of security planning by the customer
- completeness of system requirements prepared by the customer
- security education level of the system operators and administrators
- computer skills of the system operators and administrators
- availability and willingness of the customer's IT department to collaborate
- IT skill level of the integrator's project staff
- how aggressive the intended project schedule is
- how new the security technology is that's being deployed
- experience of the integrator's personnel with the technology being deployed
- leadership and interpersonal skills of the integrator's project leads

Figure 1. Project customer collaboration requirements



In spite of the significant increase in complexity, many systems integrators have not revised their strategy for executing projects. The focus of attention is most often along the lines of technology and sales-related product education. How to deal with customers is often taken on a project-by-project basis, using a trial-and-error approach. This makes it hard on both the customer and the integrator. Projects often consume more integrator resources than estimated, and schedules often extend far beyond the worst-case expectations of the customer.

Complexity Doesn't Have to Mean Chaos

There is a difference between complexity and chaos. Complex projects become chaotic (especially for the customer) when insufficient planning is performed and the integrator gets too far ahead of the customer. Technology suitability must be verified before being installed. Customer preferences must be identified before systems are configured. Education and training must be planned and designed to fit the customer's actual needs and performed at appropriate points throughout the project. These are all known good practices, but they become critical practices with convergence projects.

I discussed this subject with Emil Marone, the Chief Technology Officer of Henry Bros. Electronics, a large-scale security systems integrator headquartered in Saddle Brook, New Jersey. "Systems are growing exponentially in terms of what they can do, and what they need to do in the customer's eyes," said Marone. "Every facet of what a system can do adds that much more to scope of material and time required for training. It requires much more preparation on the part of the integrator than it has in the past. You can't just dump the full set of capabilities on the customer. You have to understand exactly what they are trying to accomplish, and present to them the most relevant options."

"One example," said Marone, "is the time a customer questioned our request to collaborate with us regarding system alarm definitions. He didn't understand why that was needed. When I printed out the full list of canned alarms—it was 34 pages long—he understood. And believe it or not, he also had a need for some custom alarms in addition to the built-in capabilities."

Marone also said, "Training is no longer a one-shot thing. Before you can collaborate with the customer about various aspects of the system, you must educate first. Often we provide several days of enlightenment for the customer's personnel, about what the system can do and the kinds of decisions that need to be made by the customer. The next step is training at the factory. What follows is highly productive collaboration about their system. Later, more education is needed before tests, and before commissioning. Last is the final formal training. There can be follow-up education as well."

Marone also pointed out the importance of educating the customer beyond the technicalities of the system. "For example, customers also need to plan for their own resource allocations," he said, "including correct staffing for ongoing system operations. They can't have only one person who knows special functions of the system. They need backup redundancy in their personnel as well their computers. So you have to understand the customer's resources and how their operations will work, in order to help them with this aspect of planning."

A well planned and highly collaborative project will insulate the customer from most of the chaos, and introduce the customer to the complexities in manageable doses. Project strategies and approaches should be developed with those ends in mind.

Understanding the Customer

Able Alarm in Louisville, Kentucky, does integration work throughout the U.S., and has a specialty in school security applications. Tom Lemely, President, explained their secret for collaborating with customers who don't really have much time for collaboration. "It's very important," Lemley said, "to understand the project from the customer's perspective. You truly have to see the project and the system from the customer's eyes, not from your own

perspective. This doesn't mean guessing about what the customer wants or going on your initial perception only."

"A big advantage for us," explained Lemley, "is that we are very experienced with school and school district applications in general, plus we also know individual schools and districts very well. We're not just collaborating for a new project ... we have been collaborating with schools on an ongoing basis for more than 20 years. We know how their individual needs have changed over time. This significantly reduces the amount of project-specific collaboration."

Lemley said, "You have to know things like, 'What are their goals and objectives? What are their constraints or limitations?'" For instance, we already know for some customers that a very non-aggressive schedule is required, to provide the kind of project flexibility that they expect. For other districts, privacy is their primary concern and security is second. Where we don't know everything we need to know, we do our homework."

You also have to identify early on who you need to collaborate with and get those customer personnel on your side. Lemley said, "For example, if you get a block of IT addresses from the customer, the IT department must respect those, or you'll have all kinds of system trouble for no good reason. That's just a small issue. We work directly with IT to ensure that both we and they understand the needs and responsibilities on both sides, and what's important or critical." Lemley concluded, "Project planning is just as much about the customer as it is about technology."

Timing

Successful project planning addresses when you plan and collaborate with the customer. If each type of planning is not performed early enough in the project, it isn't planning—it's coping. That takes more effort than real planning. It's less effective because the full attention required from each person isn't available due to time pressure and distractions. The impact: more effort but less result. This common project phrase sums it up: "I wish we had thought of that earlier."

Getting Maximum Value

Customers generally don't realize that if a project isn't going well due to a poor project approach (incomplete planning and/or insufficient customer collaboration), it's the customer who has the most power to fix it. How? By canceling the project completion date (it won't happen anyway), calling a temporary halt to the project, and initiating the kind of collaboration and planning that hasn't been happening. Don't proceed with the project until you are certain that the planning and collaboration is currently sufficient. Just one time, take the schedule pressure off and recalibrate the project. If the project personnel aren't capable enough to plan well or collaborate effectively, then get the personnel changed. If that's the case, how else could the project be fixed? Then set miniature milestones that will allow the project to be assessed and readjusted before it gets so far off course that the new completion date is jeopardized.

When planning and customer collaboration is performed to the full extent that convergence projects warrant, two very valuable things happen. First, the customer has an excellent project experience, one that continues forward in time because the system *as provided* is a very good fit for the customer's security and business operations. Second, projects are accomplished at the lowest levels of cost and schedule, and with the least strain on project personnel. Who wouldn't want that kind of project?

About the Author

Ray Bernard is board-certified as a Physical Security Professional (PSP) by ASIS International. Ray is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides high-security consulting services for public and private facilities. Ray is a technical consultant and writer who has provided pivotal direction and technical advice in the security and building automation industries for more than 18 years. For more information about Ray Bernard and RBCS go to www.go-rbcs.com or call 949-831-6788.

Read the latest articles in Security Technology & Design magazine at:

<http://www.securityinfowatch.com/cover/security-technology-design/2SIW>
