

April 2008

SECURITY

SOLUTIONS FOR ENTERPRISE SECURITY LEADERS

Goodbye Handshake; Hello Contract

As dependence on integrators increases, Tom Collins of Houston and others rely on strong contracts and relationships.

Plus: 10 Questions You Must Ask Your Integrator!

INSIDE:

- ▶ **Leading Business Technology Event: Interop Las Vegas April 27-May 2**
- ▶ **Forces of Change: Security Magazine and the Security Executive Council ID Eight Impact Trends**
- ▶ **Virginia Tech One Year Later – What We've Learned and Not**



Goodbye Handshake; Hello Contract

Tom Collins of the City of Houston works with integrators and security equipment makers in new and deeper ways.

By Bill Zalud, Editor

Especially when it comes to upgrading and new technology, project management – in conjunction with systems integrators, dealers and even manu-

facturers – is growingly important,” said Tom Collins, security manager, City of Houston/Public Utilities Division.

Collins summarizes end-user and integrator views concerning the evolution of their relationship as technology gets more complex and involves communications and

computer technologies beyond traditional security gear.

With a Ph.D. in urban and regional sciences, Collins provides leadership, sets goals and objectives for security needs for the fourth largest water utility infrastructure in the United States. Responsible for development and management of design and construction of security improvements for protection against terrorist attacks, Collins develops security routines, conducts investigations and background checks and works with the Joint Terrorism Task Force for intelligence sharing protecting critical infrastructure.

COVERING MORE TERRITORY

In a recent example, and with team involvement, Collins brought in SightLogix technology. “It covered more territory using less people. It was more reliable and allowed for a quicker, timely response to the situation on the ground.”

The technology provides intelligent video surveillance that works reliably in outdoor conditions. The enterprise security system reliably secures outdoor perimeters and buffer zones while minimizing false and nuisance alarms. Effective outdoor security requires simultaneously surmounting numerous challenges – reliable detection in all-weather 24/7 conditions, secure IT integration, simple installation and training and many more while staying within practical budgets.

For Collins, thieves were breaking into the compound and stealing assets. Thanks to the new technology and the systems integrator involvement, the new technology provides event notification in real-time.

When it comes to evaluating such gear, “There are three options for us: We can use our Engineering & Construction Division in the Public Works and Engineering Department; we can perform it in-house for smaller projects; or we can go to outside vendors to help us with project management. Our latest proj-

Emerging IP-based Solutions and the Integrator

Research suggests that companies are moving rapidly towards IP-based security solutions because of significant benefits to the client. So what should end-users look for when selecting an integrator?

“You want to ensure that your integrator has a proven track record of successful IP-based video installations, solid partnerships with leading manufacturers, and that the company inspires trust,” said Greg Lernihan, co-founder and president of Convergent Technologies.

“Consider how many years the company has been installing IP-based systems and whether it is a core competency,” Lernihan said. “Do they have the expertise to help with physical security

practices as well as networking protocols? Do they have trained and certified personnel available to design, install, service and maintain the integrity of an IP-based video system?”

“Today about 70 percent of our camera installations are IP-based,” said Dan Mocerri, Convergent co-founder and chief executive officer. “Several years ago we recognized that the security industry would be rapidly migrating to IP-based video. We began to invest heavily to certify our team in IT practices, and we also aggressively began recruiting people with IT backgrounds.”

Selecting an integrator that shares a similar culture and value system with the customer’s organization is another key to building a long-term, successful partnership, Lernihan said.

ect for security improvements is being managed through an outside vendor.”

DIVERSITY OF TECH, SERVICES

Said Collins, “Budgets are tight, government budgets are tighter. The water industry is regulated by the EPA at the federal level, and by the Texas Commission on Environmental Quality at the state level. Each level, the state and federal, follows closely our continuing security improvements. The EPA has a record of our vulnerability assessment, and though it is not yet a requirement that we must implement each and every recommendation in the assessment, liability issues, should an event occur, would cause a reasonable person to provide an improvement implementation plan showing continuous improvement. This is something we are achieving in the Public Utilities Division in spite of a limited budget.”

His security section uses metrics for identifying and assessing the vulnerability of the utility’s critical infrastructure and key assets and it also uses a metrics-based system of performance evaluation.

COST AND RISK

“Our metrics allow us to assign a cost per risk reduction unit (RRU). We can have RRU/costs based on capitol improvements, as an annual average, or as a scenario based on proposed improvements. This gives upper management actionable information for a rational decision. Security costs can then be weighed against other costs such as maintenance, IT upgrades, or even equipment purchases. Within the security section, we use RRUs to determine where our dollars go furthest. For instance, private security officers cost more per RRU than the installation of edge perimeter devices with video analytics. We feel that with a central

A Strong Foundation Is the Key

How many times have you heard that a strong foundation is the key? It goes without saying that a strong foundation is most often the first key measurement of success for just about everything we associate with on a daily basis. Our homes, our businesses and our lives would be a disaster without a solid foundation, according to Rob Hile of Adesta.



“As I meet with today’s end-users, I am often times amazed at the level of research that they have conducted on different technologies that exist in an effort to get the very best security protection available. That same level of effort needs to be put into choosing their systems integrator. Having an integration partner who is competent in communication networks is the only way to achieve a solid physical security system.”

“In this era of convergence, a strong network infrastructure or communications backbone is an essential foundation,” said Rob Hile of Adesta.

dispatch and the perimeter edge devices connected to an operations center we can cover more geographic area with fewer people.”

In West Palm Beach, a systems integrator with wireless expertise works with the city and law enforcement in a win-win situation.

SPECIALTY INTEGRATORS

Security 101 of Fort Lauderdale, Fla., designed and implemented the system after winning the project in a rigorous request for proposal process. “We have been in the wireless surveillance business for over three years and had prior experience with Firetide,” said Jim Letang of Security 101. The entire mesh and access network for the City of West Palm Beach was deployed in just two days.”

The West Palm Beach Police Department now has “digital eyes” on the streets. The police department has set up an advanced wireless video surveillance network working under the supervision of the West Palm Beach Police Department; screened

and trained civilian monitors will join a 400-strong police volunteer force to monitor real-time video feeds and alert police dispatch of any incidents.

“Video surveillance is another important tool in the fight against crime and our efforts to protect the public,” said Assistant Chief of Police Willie Perez. “The system is a great ‘officer safety tool’ as well. For example, we have a request from a bank to join our wireless network, giving us visibility into the interior of the bank as officers are responding. So our officers will know what they are facing before they arrive on the scene. The capabilities of the system are fantastic, and we are just scratching the surface of what Firetide technology makes possible.”

In the first phase of the network, the West Palm Beach Police Department set up a 13-camera system focused on the toughest neighborhoods in this city of 100,000 residents in an effort to deter gang activity, drug dealing and prostitution. Seventeen mesh

Fighting Budget Constraints with an Integrator’s Help

Budget constraints are always going to be a challenge, but new technologies offer ways to leverage investment that changes the traditional profile of security spending. By automating previously manual tasks, staff can be optimized, resulting in labor cost reductions. For example, instead of having a group of security officers watching cameras, video analytics can watch for anomalies and alert officers when they’re detected. And digital video is allowing consolidation of security camera monitoring from multiple locations to fewer, more concentrated locations, sometimes hundreds or thousands of miles away from the location being monitored, according to David Gupta, CEO and president of SD-I.

“Today, staff needs to be more technically skilled than ever before. Technology is infiltrating every aspect of security, requiring security staff to be comfortable using technology in their daily

work. Computer skills are becoming a necessity, which is driving the growth in outsourcing, since it provides access to a larger pool of talent and greater flexibility in staff size,” said Gupta.

According to Gupta, effective project management has grown in importance as a result of the complexity of the systems that security managers are implementing. Unlike the past, where systems were not integrated and were comparatively simple, today’s security systems are computer-based, integrated, and require far more sophisticated skills. This means that there are more disciplines involved, the planning is more complex, and the consequences of failure are greater than ever before.

Security projects typically involve four very diverse groups with widely varying perspectives and objectives: security, facilities/construction, operations, and information technology.

nodes connect the cameras to police headquarters, where video can be accessed by dispatch personnel and stored for evidentiary purposes. Each mesh node is coupled with an access point to allow access to video feeds from Wi-Fi-enabled laptops in police cruisers, providing real-time situational awareness as officers respond to calls for service.

CHANGE IN RELATIONSHIP

For Jesse Fecteau, vice president of corporate security for Lehman Brothers, he also sees a change in working with systems integrators. "My group looks into and deploys new technologies to address security concerns at the firm. We are working on products such as GPS tracking of employees who travel in

certain countries, RFID for evacuations, IP video, video analytics, Mumbai bus tracking and intrusion detection on various access points in the firm. Prior to Lehman I spent 10 years in the IT world as a network security engineer. I am utilizing past IT experience to leverage the changes in technology in the physical security space."

With this background, Fecteau believes he is actively changing "our relationship with our integrator in terms of how they help us deploy new technologies, as well as getting the right people to support us from the IT side of the industry." To him, knowledge in networking, databases, script writing, etc., is important. "Most new technologies will be researched by my group and



The West Palm Beach Police Department now has "digital eyes" on the streets. The police department has set up an advanced wireless video surveillance network, said Rich Montalvo of Security 101.

Building and IT Systems Come Together

According to John Gnadinger of Johnson Controls, Inc., "Prior to 9-11, it was uncommon to integrate security with building and IT systems. Today, all that has changed. Systems like access control, security video and perimeter security all feed into central monitoring and management software. Facilities are integrating security technology with building, IT and end-user systems to enhance business applications and energy efficiency, as when access control is integrated with lighting and comfort controls to save electricity when the building is unoccupied."

As security technology has evolved so too has the role of the security integrator. Today's integrators neither shoehorn custom-

ers into proprietary solutions nor exist in "security only" silos. The integrator's job is to analyze the customer's business needs and provide best in class solutions. The process begins with a solid analysis of the customer's business needs. Then the integrator develops converged technology solutions to meet those needs.

Said Gnadinger, "When looking for an integrator, look for three things: experience, engineering acumen and someone who understands your business. Experience means having a process for working with the customer. An experienced integrator will bring a methodology to the project for planning and design. Experience with a broad array of technologies, solutions and platforms gives the integrator useful toolkit to address the facility's challenges."

10 Qualities Your Systems Integrator Should Have

According to Noelle Britton of Siemens Building Technologies, Inc., you should expect that your integrator will guide you toward a custom solution tailored to meet your needs.

1. Desire to develop long-term partnerships. The strength of an integrator is measured by the ability to develop long-term strategic partnerships with you.
2. Segment-specific knowledge. It is imperative that your integrator knows your business as well as you do.
3. Certification. Your integrator should promote a culture of continuing education that focuses on bringing value back to you, the customer. Certification assures you that the integrator's staff has a deep knowledge of the industry and products/platforms.
4. IT/IP knowledge. With the convergence of physical security and IT, and the abundance of IP products on the market, your integrator must know how to converge these two silos.
5. Exceptional customer service. It is not enough for your integrator to simply design and install your security system.
6. Broad organizational capabilities. Your integrator should have the capabilities to deliver a solution on a global, national level and a local level. Integrators with such breadth can share best demonstrated practices between staff and across regions and markets.
7. Best-in-breed portfolio. Security integrators need to have a robust portfolio of best-in-breed products that can accommodate different customers.
8. ESP. While no one can predict the future, your integrator should keep a watchful eye on how your business grows and evolves so that your security solution adapts with it.
9. Financial stability. You are increasingly making purchasing decisions based on a longer-term perspective. To that end, you should take into account the stability of an integrator.
10. Industry knowledge. It seems obvious, but you'd be surprised at the number of integrators who don't have an extensive knowledge of the industry.



You should expect that your integrator will guide you toward a custom solution tailored to meet your needs, according to Noelle Britton of Siemens Building Technologies.



For Jesse Fecteau, vice president of corporate security for Lehman Brothers, there is a real change in relationship with systems integrators.

brought to the integrator when it's time for a deployment. The old model seemed that the end-user asked the integrator for a solution to a certain problem, and then the integrator came back with a solution. We have changed that model somewhat at Lehman.

"We only use one integrator (Securitas Systems). PEI prior to that but Securitas acquired them so we don't really have questions that we ask them prior to a job. They are our guys, and we are working more on integrating their skills and people into our team, rather than just throwing jobs at them. Their knowledge of navigating around Lehman is very important to us -- who to talk to for certain issues, our culture, politics, etc.

"Being that we are one of the big global investment banks, our budget is tight this year due to the sub-prime issues and massive Wall Street write downs. We hope to see that change over the next year or two. However, we have partnered up with other business units to provide more services to their needs. For instance, HR asks us to give them data on people working excessive hours in a week. Some people, based on their IN/OUT swipe data put in between 80 – 100 hours a week. After a while they may get burned out and leave the firm. This is a concern for HR and the specific business unit."

KNOWLEDGE OF THE COMPANY

On the people side, Fecteau said, "As most firms might agree, we would like to retain people in our security group. Over time it's not just the knowledge of products and security that is helpful, but also knowledge of the firm's operations, key people, sensitive locations. It takes a good year or two before someone can really move around Lehman effectively to get things done. A good portion of the positions are promoted within."

It's the same thing with a systems integrator relationship. **SECURITY**

What End-users Should Consider When Considering an Integrator

Security Magazine asked end-users and consultants what they think are the important ten questions to think about when considering a systems integrator. What follows are four examples that reflect most input.

From Will Dettmering:

1. What is the current network topology?
2. What do you want to accomplish with your proposed network security/surveillance project?
3. How old is the current network?
4. What is your network software system?
5. What is the current network's capability and capacity?
6. Do you require mirrored/off-site storage of data?
7. How long do you plan on depreciating your equipment?
8. Do you have centralized or distributed monitoring and management of the system?
9. What is the timeline you require for installation, testing, and user education?
10. What is your proposed budget?

From Robert M. Wetherell, CPP, CFM, Manager, Facilities - Cedar Rapids Processing Pearson

1. If software, is this proprietary or off the shelf software?
2. What are on-going maintenance costs?
3. What will be necessary for future upgrades?
4. Has this been accomplished in other applications and what were the results?
5. Are there other more efficient/economical options?
6. How will this affect my energy consumption/carbon footprint?
7. How will this affect my bandwidth?
8. What training/support will you provide and what is the cost?
9. What is the next generation of this technology?
10. Give me 10 reasons why I should choose you as my integrator for this project.

From Roger Rangel, Goodwill Industries International, Loss Prevention and Safety

1. Can you provide me with your technicians' technical experience and how long has he/she been with your company?
2. Please provide me with references and direct name contact.
3. What is the longevity or life expectancy of the product you are recom-

mending?

4. What is the software updates scheduled for the product in question?
5. As a result of the software updates will there be additional fees for any changes?
6. When was the product manufactured?
7. May I see the warranty?
8. Can you provide me with samples of your latest project that met expectations?
9. Can you provide me with samples of your latest project that did not meet expectations and why?
10. Ask for a detail report of the contract work and product information.

From David Oliver, Cadbury Adams

1. What background checks are conducted on your staffers prior to hiring as a condition of employment? (i.e.: criminal, financial, credit, past employment etc)
2. What training, educational background or certifications do your technical staffers hold and are they valid?
3. Do you stand behind the products and services you sell/market and do you honor hardware makers' warranties or facilitate any warranty claims on the client's behalf.
4. What is the level of IT expertise and system integration your technical staff have and support. (i.e.: database management, SQL, Oracle, network architecture, MS Certified System Administration, CISCO system or network admin)
5. How long has your organization been in business and is its primary focus on security?
6. How large is your organization, is it financial stable and can you handle larger projects?
7. What other value added services does your organization provide?
8. What are your service & support plans like? Also, what are typical response times should a critical infrastructure device fail and requires repair or replacement?
9. Show us several other installations similar in nature to the system we have deployed or plan to deploy. Also provide us with a contact person for reference purpose at several client locations.
10. What brand of products do you primarily recommend and support? Are you willing to provide products and offer support for what the end client has specified if it is different from what is typically utilized?



SightLogix, Inc.
745 Alexander Road
Princeton, NJ 08540
609.951.0008