

The Perfect Partner

By Diane Ritchey, Editor

It's a partnership that can succeed or fail, and many factors are in play in determining the outcome. Of course, security integrators want you to "communicate" with them upfront and go beyond the final hand-shake. But what else makes a perfect relationship, and what are they thinking about you?

We asked the top security integrators based on a ranking from sister publication *SDM*, to tell us about their brightest customer, what they learn from the security directors whom they work with each day, the most dynamic sector of the industry in their minds and more. Our



"Our brightest customers understand their organizations' values and core competencies," says Carey Boethel of Siemens Security Solutions.

participants include Christopher BenVau of Stanley CSS, Carey Boethel of Siemens Security Solutions, Thomas J. Giannini of SimplexGrinnell, Jay Hahn of ADT Security Services, Ed Meltzer of Niscayah, Inc., Michael Mann of Johnson Controls, V. John Stroia of Diebold, Incorporated and Tony Varco of Convergent Technologies.

Security magazine: Who is your brightest security customer, and how have they achieved that honor?

Carey Boethel of Siemens: "Our brightest customers understand their organiza-

tions' values and core competencies. They know what they do best, and they know what their partners do better. They rely on their partners to help create value within their own organization, ultimately allowing them to focus on their core business.

For these customers, price is not the sole reason they decide to partner with a systems integrator. They look at the value that the integrator will bring to their organization. Will the integrator's value proposition allow me to focus more on my core business? Will the integrator help optimize my processes and procedures to ensure I am getting the most of my security solution? Is the integrator forward thinking and able to forecast my security needs well into the future?"



"We often encourage customers to balance their appetite for cutting edge technology such as pure IP plays with more pragmatic considerations such as cost and performance of those technologies," says Christopher BenVau of Stanley CSS.

Tony Varco of Convergent Technologies:

"Our brightest customers are those who properly identify and analyze the security challenges they face, have worked closely with Convergent to evaluate and understand the various technologies that could solve a particular problem, are actively involved in the implementation of the solution, are interested in establishing metrics to measure results and understand the importance of properly maintaining systems once they have been installed."

Christopher BenVau of Stanley Convergent Security Solutions, Inc.: "One of our brightest customers is Cisco Systems, a leader in the technology space for their customers and in leveraging technology within their own facilities and works spaces. As Cisco's systems integrator for the Americas, Stanley CSS implements a high level of integration, which includes their IT infrastructure, human resources and logical security. Stanley is also a Cisco ATP and global telepresence user."

V. John Stroia of Diebold: "A recent example of our customers' innovation is the National Oceanic and Atmospheric Administration (NOAA). Since 2009, Diebold has partnered with NOAA to set the groundwork for streamlining the agency's identity, credential and access management (ICAM) across its entire enterprise, as well as to ensure the interoperability of its physical and logical access control systems (PACS and LACS).

NOAA has taken a progressive position when it comes to ICAM, and the agency is truly at the forefront of the ICAM initiative. In working with NOAA, Diebold has had the opportunity to play a consultative role, which is where leading integrators can deliver real value."

Tom Giannini of SimplexGrinnell: "Our brightest customers are those that participate in the entire process to source integrated systems. They are knowledgeable of their needs, forward looking and establish criteria that potential system integrators must achieve. They are engaged from the inception of their project through the life cycle of the investment in the life-safety or security solution installed. One of our customers who best represent these attributes is Youngstown (Ohio) State University. YSU's senior leadership team took an innovative approach in creating an emergency communications system that not only serviced the large urban campus, but included key off-campus locations such as privatized student housing and retail establishments as well."

Ed Meltzer of Niscayah: "Our brightest customers are the ones who allow us to leverage our knowledge and experience and per-

mit us to manage and service their systems with their business drivers in mind. The reason is that we are permitted to do our job and our customer acknowledges our expertise and experience with the many different facets of the systems integration environment. That level of trust and cooperation rightly delegates the proper scope of work to Niscayah and allows the customer to focus more on their core responsibilities.”

Michael Mann of Johnson Controls: “Our brightest customers understand the short and long-term benefits of sound systems integration. They see why building automation and business systems must work in tandem with security systems. This linkage can maximize the protection of people, property and assets while reducing energy use and increasing operational efficiencies.

One example is Ave Maria University in southwest Florida, where executives wanted to increase the safety and comfort of all buildings on campus. University administrators were able to reduce energy costs through the integration of occupancy sensors with the lighting and HVAC systems. As a result, lighting and airflow are activated in rooms and lecture halls only when needed. The system integration particularly benefits the fire and life safety response. If the alarm system detects a fire, the HVAC system is signaled to stop delivering fresh air to the area and pressurizes the path of egress, clearing it of smoke. The access control system will unlock doors along the emergency route and real-time surveillance cameras will give responders a live feed in the event of a fire emergency.”

Security magazine: Beyond asking security directors to communicate with you and to involve you more, what advice can you give them to ensure that they are installing the correct technology, that it will work and you will have a successful long-term partnership?

Jay Hauhn: “You need to know what keeps your customer awake at night. Once you understand the security challenges he or she faces, it is a matter of applying technology and services to mitigate those risks. Working with an integrator you trust and one that has the proper skills and knowledge to execute is crucial.”

Tom Giannini: “We recommend they do their homework on the technology they want to use. We can assist them with that selection, or depending on the customer, we will encourage them to hire a consulting firm to provide that guidance. They should also establish the business, performance and financial criteria for their proposed systems

integration provider. We have developed a one-page tutorial for our potential customers on how to select a systems integrator, which can assist with this critical decision process.”

Carey Boethel: “It’s important for our customers to embrace standards such as ONVIF in order to lower the total cost of ownership and thereby create value. Standards help ensure compatibility between disparate systems, which allows the security solution to evolve as the customer’s organization does.”

Ed Meltzer: “The best advice we can offer our clients is to reflect on what their core business drivers are and how they relate



“In any sector of the economy, the basics of good relationships begin with people and communication,” says Ed Meltzer of Niscayah.

to the problem they are trying to solve. Is it a technology, operational or process related issue? Does the problem they are trying to solve and the solution possibly impact others? And also, what are the TCO considerations? Careful reflection of these considerations will preempt the application of inappropriate or ineffective solutions, technological or otherwise.”

Tony Varco: “End-user customers must take an active role throughout the entire process, and work (up-front) with a qualified and experienced systems integrator who can facilitate the process from start to finish. This includes conducting professional vulnerability assessments and creating a formal physical security implementation plan, assessing technology by facilitating demonstrations between multiple product manufacturers, asking for and checking references where a particular solution has been implemented and lastly ensuring the systems integrator is properly certified to install and service the solution.”

Christopher BenVau: “We encourage our customers to collaborate with other departments within their business sharing business

objectives and growth plan. This is crucial as gone are the days of security operating as a separate channel. Now, changes in business operations, human resources, facilities, legal and even marketing will impact the structure and expectations for physical security. We often encourage customers to balance their appetite for cutting edge technology such as pure IP plays with more pragmatic considerations such as cost and performance of those technologies.”

V. John Stroia: “Today, security has to be about more than upgrading equipment. It has to go beyond what’s tactical. Successful security engagements take into



“Today, security has to be about more than upgrading equipment,” says V. John Stroia of Diebold.

consideration business issues. They deliver on specific objectives. And they have reach beyond the security department to provide value for the entire enterprise. Identifying the correct technology requires thinking that goes beyond the equipment itself.”

Security magazine: What has been your favorite security installation to date and why?

Tony Varco: “Our favorite installation involved a large logistics customer that installed technology to streamline operations, improve quality and provide a tangible return on investment. What made this particular installation so interesting is that we were able to track the hard savings generated and provide the clients upper management team with proper justification for making the investment.”

Christopher BenVau: “With the eyes of the world watching, it was a great honor for Stanley CSS to partner with Bell Canada during the Olympic Vancouver 2010 Winter Games. Stanley CSS was responsible for securing numerous critical sites that were equipped with the first all-IP Games network, the biggest Olympic network of all time.

Stanley CSS worked with Bell Canada to provide temporary access control systems on their mobile telecommunications trailers which contained the equipment to support this increased demand for telephone and internet communication during the Olympics. A unique cellular network was developed and tested to provide data communication between these trailers and their existing access control system platform as well as portable wireless security controllers were packaged into carrying cases to provide a mobile solution, which were able to be powered from a vehicle cigarette lighter adaptor.”

V. John Stroia: “Every installation has its own unique attributes, and each enables us to enhance our expertise. But one recent engagement stands out because of the opportunity it provided to even further elevate our focus on quality.

Diebold’s LINX Predator Elite Integrated Security System is now in place at a nuclear weapons storage facility for the U.S. Air Force. The facility is among the most highly guarded and protected U.S. Military sites, at Protection Level 1 (PL1). Diebold’s solution is the only of its kind to be approved for use at this type of military facility.

This installation was unique and technically challenging. And it came with the strictest of requirements and specifications. Because the facility is designed to protect the most important military assets on the planet, it demanded flawless performance by the Diebold team. There was no tolerance for failure. Every detail of the installation had to hit the mark – 100 percent.

The Diebold solution seamlessly integrates all security functions at the facility, enabling complete control and monitoring of the entire site from a single command-and-control station. Our successful execution of this project will have a long-term impact on the quality of Diebold’s security solutions and services. The needs of this particular installation and customer required us to be even more meticulous than ever before. It required a new level of innovation on the part of our security experts.”

Ed Meltzer: “I would nominate a large telecommunication project with several thousand readers and an equal number of cameras across in a national project deployment. The project has demonstrated to the customer that we could leverage the value of the technology to increase security, reduce risk and improve business performance. Furthermore, it demonstrated that a programmatic approach to support and service works well, especially in such a

geographically and technologically diverse system.”

Carey Boethel: “We are currently working on a citywide surveillance project for one of the largest cities in the U.S. This project is particularly exciting because of the changes to our society that are happening as a result of urbanization and demographic change – these two megatrends are driving demand in this space and the work is very rewarding. We are creating a safe and secure environment for the city’s inhabitants, which make a difference in people’s lives.”

Jay Hauhn: “Early in my ADT career I worked in our Federal Systems group and did a lot of work with the United States



“You need to know what keeps your customer awake at night,” says Jay Hauhn of ADT.

government. Designing and implementing security systems for federal government locations was both fun and, professionally very satisfying. ADT continues to do considerable government work and while I do not personally get involved in many of the projects, they remain my favorite because of the sophisticated nature of the technologies that are used.”

Security magazine: What is your biggest challenge with working with an inexperienced and an experienced security director? What do both of them bring to the table?

Tony Varco: “The biggest challenge is the amount of upfront education that is required. Before the Security Director is able to internally position and ‘sell’ the project to upper management, it’s imperative that he/she has a complete understanding of the solution and associated features/benefits to the organization, including a return on investment. An experienced Security Director understands that their projects are competing with others within the organization. This being the case, they will include a

financial justification, within the proposal, that provides a detailed and realistic return on investment. The inexperienced Security Director we work with typically brings high energy and a fresh approach to the table.”

Michael Mann: “Regardless of the security director’s experience level, it is vital that he/she understands the value of holistic planning with their peers throughout the C-level. The demand for improved business outcomes from better efficiency does not fall solely on security decision-makers. Rather, building system integration needs to be top-of-mind for all key decision makers. The current economic environment is an ideal time for facility managers, department leads, and building owners to take a holistic



“Regardless of the security director’s experience level, it is vital that he/she understands the value of holistic planning with their peers throughout the C-level,” says Michael Mann of Johnson Controls.

approach to building planning and management that includes maintaining secure building environments.”

Carey Boethel: “The challenge with inexperienced security directors is that they want to do everything because they believe doing so creates job security when in fact creating value and contributing to the company’s bottom-line produces that job security. These security directors are not as open to partnerships as a more seasoned executive might be.

The challenge with experienced security directors is the tendency to do things the same way over and over again. They can be slow to adopt new, innovative ways of solving problems. Both bring with them opportunities to demonstrate value.”

V. John Stroia: “When working with an inexperienced security director, integrators often have the opportunity for an even higher level of involvement in the security initiative. Newer directors may view

the integrator in more of a consultative role, allowing the integrator to provide a great deal of guidance when it comes to specifications, regulation, best practices, technology, etc. Rookie directors, in general, also tend to be open to innovation.

On the other hand, experienced security directors often have the internal relationships needed to ensure funding and support for security initiatives. Veteran directors are more likely to already have earned the trust of others within their organizations, and they typically have the internal contacts and buy-in needed to give security more visibility on an enterprise level.”

Tom Giannini: “Many times an inexperienced security director will try to use



“Technology supplements a customer’s security program and plans; it cannot supplant that program,” says Tom Giannini of SimplexGrinnell.

technology to overcompensate or solve issues. Technology supplements a customer’s security program and plans; it cannot supplant that program. In these cases we work very closely with a new security director to fully understand the program, what the technology needs to achieve and how we can incorporate the technology to make their security program more complete. An experienced security director will be more knowledgeable about the technology available and how it needs to align with their security program. In these cases our first priority is to ensure the customer gets vetted technology, and that we do not encourage them to acquire technology that has just emerged in the marketplace. Our industry has technology advancements occurring on a regular basis, but we must be careful not to connect a customer with a technology platform that is not yet ready for primetime.”

Christopher BenVau: “Working with an inexperienced security director often requires a greater investment on the inte-

grators part in identifying gaps in current process and systems. In addition, it is important to take the time to demonstrate available technologies and solutions to the client. If executed properly this builds a strong partnership between the client and integrator allowing the provider to take the lead on recommendations for solutions.

Many experienced security directors with the proper internal resources will identify their gaps in process, formulate a solution and even specify the technology and platform to implement. While the integrator’s input is still important, it is important to respect the client’s opinions and preferences. These experienced security directors are a great source of information for integrators that are willing to listen and learn from the end user’s perspective. Some of our most unique solutions have come from these industry professionals.”

Ed Meltzer: “The experienced security director possesses a mature view of the interrelationships between physical, electronic and investigative components of a corporate security program. They bring an understanding of the roles and relationships of the service providers and can articulate their needs proportionately to the involvement of the providers in their programs and the degree of risk associated with that component of their overall security plan. There are fewer challenges in these relationships.

The inexperienced security director may not yet possess an understanding of the value of strong vendor relationships and may rely too heavily on a particular independent management strategy. This tends to foster a reactive approach to problem solving and day to day operations. This puts an inordinate amount of pressure on the providers and encumbers our ability to help manage our portion of their programs. That being said, the inexperienced security director customer presents an excellent opportunity for the integrator to demonstrate their value over time.”

Security magazine: Is there one sector of the industry that is more difficult and why? Is there one that’s easier to work with and how?

Carey Boethel: “Any sector that faces strict regulatory requirements can be more challenging. Because of the fiduciary duty that we assume in ensuring that the security solution is in compliance with regulations, mandates, etc., it’s important for security directors to partner with a systems integrator that has the vertical market expertise to fully understand and apply the industry-relevant regulations to their security operations. Non-compliance can cost a company millions of

dollars in fines and lost revenue.”

Christopher BenVau: “Some of the more challenging customers come from the emerging technology sector. By definition they are exposed to the most cutting edge technologies and their expectations of electronic security systems often test the limit of the industry offerings. The keys to success in this channel is being current in the IT space, having team members certified on industry standard systems, and having a grasp on all available electronic security offerings. In the cases where the requirement cannot be met with current offerings, Stanley CSS’s Enterprise Solutions group custom engineers technologies such as our Corporate Commander platform.

Retailers tend to have the largest and most mature Loss Prevention (LP) departments as shrink and risk mitigation is key to profitability. These internal LP teams take a significant burden off of the integrator as they often have internal training for associates, field LP professionals and a refined security process. This often makes new solution delivery easier than other sectors. That said, retailers often challenge their security vendors to provide cutting edge solutions and the lowest possible investment making retail a highly competitive space.”

Ed Meltzer: “We don’t believe there is any one industry that can claim to be the winner of this prize. In any sector of the economy, the basics of good relationships begin with people and communication. It is absolutely critical that we understand our customer’s business drivers and that we approach them with solutions in mind, not widgets.”

Tony Varco: “The reality is that each vertical market has its own unique set of challenges. One of the more challenging vertical markets to work with is the federal government market. It’s important to clearly understand the process, execute the required documentation and have the proper certifications required to bid and compete on these projects. Integrators who leverage GSA contracts to secure this type of government work also need to properly document and track projects for audit purposes. I would say it’s not necessarily easier to work with one particular vertical market over another, as each market has its challenges and nuances. However, it is easier to work with certain end-user customers versus others. Customers who are trained, educated and actively involved in the process tend to be easier to work with than those who are uninvolved and detached from the process.”

Michael Mann: ‘It is fair to say that each and every vertical sector presents a unique set of opportunities and challenges. We believe that it’s vital to have extensive vertical market expertise to address the specific policies, compliance and industry business processes to meet any customer’s desired business outcomes. The integration needs of a hospital are vastly different than a public school system.

We can take this debate a step further and

consider the global variances of the customers we provide integrated security solutions to around the world – each region with its own unique sets of needs versus wants.

What we have discovered is that while security is globally viewed as the need to protect life, property and assets, the one-size-fits-all approach that some security providers market cannot work all regions.”

Tom Giannini: “We do not believe there is any one market that is more difficult

than another to support and service. It is incumbent upon us as integrators to know our customers’ prime business, how their security and life-safety programs support their business operations, and how we can supplement their success with our products and services. In many cases a vertical market that is more regulated can actually be easier to support because it provides standards that must be achieved.”

V. John Stroia: “Today, each market has

The Participants:

Christopher BenVau has 18 years of security industry experience and has a background working in sales, sales management, operations, PnL responsibility and executive leadership. BenVau believes in setting high standards, leading by example, being visible, accessible and staying in front of the competition. He works out of the Stanley CSS Field Headquarters in Naperville, IL. He has been with Stanley CSS for five years.

As vice president and business unit head, **Carey Boethel** is responsible for the day-to-day operations as well as the financial and competitive success of Siemens Security Solutions Business Unit. An industry veteran, Boethel has more than 17 years of hands-on security sales, operations, executive management and consulting experience. Boethel joined Siemens Building Technologies in 2008 as Senior Director, Business Development. Prior to joining Siemens, Boethel was Division Vice President for Houston-based NetVersant Solutions, Inc., where he held leadership and P&L responsibility for the company’s Electronic Security Systems business. He is a member of ASIS and is a Certified Protection Professional, as well as a member of the SIA Board of Directors.

Thomas J. Giannini, director of security and emergency communications marketing at SimplexGrinnell, has more than 30 years of experience in the security and life-safety industry. A Certified Protection Professional since 1997, Giannini has been involved in security management and security operations, both domestically and internationally. He has considerable expertise in the area of campus safety and preparedness, authoring numerous articles on that topic for trade magazines. Giannini came to SimplexGrinnell in 1996, and in his current position is responsible for strategic development, business planning and marketing for integrated security and emergency communication systems. Prior to joining SimplexGrinnell, Giannini worked a total of 15 years as a corporate director of security for Raytheon and Sanders Electronics. He also spent 10 years in the military, where he served in the Military Police Criminal Investigations Division, Counter Terrorism Operations.

Jay Hahn serves as chief technology officer and vice president of industry relations for ADT Security Services, the world’s largest provider of electronic security services. In his current position, he oversees and helps evaluate new and emerging security product technologies and serves as ADT’s lead executive responsible for industry relations. Hahn has more than 30 years of security industry experience, having joined ADT in 1977. He also served briefly as an executive director with Tyco Safety Products. Earlier this year, the Security Industry Association presented Hahn with its Statesman Award for his advocacy efforts on behalf of the

security industry. He is a member of SIA’s Board of Directors, Executive Committee and its Government Relations Committee. Hahn also serves a board member of the Security Industry Alarm Coalition (SIAC) and the Central Station Alarm Association (CSAA). He is chairman of the Electronic Security Association (ESA) Government Relations Committee.

Michael Mann is the director of global solution development for the Security and Fire Solutions business within Building Efficiency for Johnson Controls. Mann joined Johnson Controls in July 2007 and is responsible for solutions development, strategy and marketing. Most recently, Mann was the director of global industry marketing for Rockwell Automation, and prior to that he was director of global marketing for IBM where he was responsible for solution development and marketing, brand management, communication, and market segmentation.

Ed Meltzer serves as the national director of system management for Niscayah, Inc. With more than 30 years of experience in the security systems integration and wireless industries, Meltzer now leads Niscayah’s national service program. His primary areas of responsibility are to create, define, plan, and direct service offerings and customer service activities nationwide for Niscayah. Meltzer also participates in and is a member of Niscayah’s International System Management Group which is comprised of service leaders from all 16 countries where Niscayah has a presence and represents the U.S. in the Niscayah International Communications Group.

V. John Stroia is vice president, enterprise security solutions, for Diebold, Incorporated. He is responsible for leading a team of 500 associates focused on providing secure, integrated solutions to retailers, commercial facilities and government agencies. In addition, Stroia currently serves as vice chairman of the Security Industry Association’s (SIA) board of directors. The organization recognized Stroia as its 2009 Chairperson of the Year for his service to the industry as one of SIA’s committee chairs. Stroia joined Diebold in 1991 as an intern. He later became a product planning specialist with InterBold®, a partnership between Diebold and IBM. Throughout his career at Diebold, Stroia has held numerous management-level positions in Ohio and North Carolina, including marketing manager for the financial industry and national account manager.

Since May of 2001, **Tony Varco** has been the vice president of security for Convergent Technologies, a North American Systems Integrator with 25 locations and more than 775 colleagues. Tony is a twenty-three year industry veteran and has helped to build Convergent into one of the premier IP-focused systems integrators in North America.

its own set of challenges. In government and critical infrastructure, end-users are adapting to evolving regulation. Retailers have to find new ways to fund vital security initiatives. Educational and healthcare organizations are working to maintain their open, accessible environments while protecting their patients, students, employees and visitors, as well as sensitive information. And financial institutions are responding to unprecedented change in their business environments. From this perspective, no one market is more challenging than another. Regardless of the market, today's end-users are addressing similar business issues. They're looking to Diebold to help them enhance security and mitigate fraud. And while we're working together to anticipate and mitigate ever-evolving threats, we're also looking to improve operational efficiency. These business issues – enhanced security, the mitigation of fraud and improved operational efficiency – are a common thread from market to market.”

Jay Haubn: “I don't believe any vertical market is more difficult or easier to work with than any other. Each vertical has a number of security threats that are unique to them, as well as the typical challenges that confront all security directors. The down economy has put particularly strain on loss prevention professionals in retail. Reduced retail spending by consumers has resulted in the tightening of retail security budgets. However, at the same time, retailers are faced with increasing attacks from Organized Retail Crime gangs.”

Security magazine: Is there one sector of the industry that is more dynamic than others? And is that related to how much funding it receives?

Michael Mann: “The education and government sectors are under a growing amount of pressure to optimize their security and building management processes. When you consider recent global events, these sectors must take additional measures to prevent and manage risk. Strict compliance regulations and preventative measure are being called for and introduced into these markets. It's an ever changing landscape that requires industry expertise, technology innovative and adaptability.”

Carey Boethel: “Critical infrastructure is dynamic because of the changing needs for security in that sector. Even a small security breach can create a ripple effect that has a lasting, downward impact on economic stability; local, regional, or national prosperity; and national security. In 2007, for the first

time ever, more people lived and worked in cities than in rural areas, and the United Nations estimates that the world's urban population will increase from 3 billion today to more than 5 billion by the year 2030. As more and more people move from rural to urban areas, the strain on our nation's critical infrastructure increases significantly.”

Jay Haubn: “The Federal Government space is often on the leading edge of technology requirements because of the extremely sensitive and classified nature of the work they do. Often the technologies developed and implemented for our government customers are adopted and adapted for other sectors of the commercial marketplace. Banking is another example of customers who have so much at stake that they need the latest technologies and services security can provide. Financial institutions are increasing relying upon ADT to provide the kinds of instant access to high resolution video coupled with access control. The dynamic areas of growth are often driven more by business needs and a proven return on investment.”

Tom Giannini: “We believe there are some vertical markets that have more funding available currently than others. But this is the ebb and flow of many industries, not just life safety and security. An integrator must understand the customer's prime business, know the funding processes or programs available to support their security and life-safety programs, and work with them to help maximize the available funding.”

Christopher BenVau: “The high security segment of the federal government is a dynamic space. These customers typically use emerging technology in a highly regulated space. With the continued global terror threat funding at a historic high and the missions extremely critical, only the most sophisticated integrators with a firm grasp of federal procurement rules succeed in this space. Stanley CSS's Federal Program provides dedicated Account Managers, Application Engineers and Program Managers in our Washington D.C. office providing solutions and services to both Federal Government end users and contractors.”

Tony Varco: “The federal government sector and vertical markets such as utilities and petrochemical that are subject to federal compliance regulations tend to be more dynamic and certainly in a growth mode. Funding definitely plays a role in determining how active a particular sector of the market is. However, regulations and compliance tend to play an even bigger role



“Customers who are trained, educated and actively involved in the process tend to be easier to work with than those who are uninvolved and detached from the process,” believes Tony Varco of Converjint Technologies.

in driving these particular markets.”

Ed Meltzer: “In our experience the healthcare industry presents a very dynamic environment. Funding has less to do with the dynamics of the business than regulatory oversight, variation of risk and the public's role in addressing the challenges associated with securing facilities.”

V. John Stroia: “The most dynamic market today – in terms of the rate of change it is experiencing – is critical infrastructure. Many events of the past decade, especially September 11, have heightened our awareness of the vulnerability of our nation's airports, rail/subway, ports, power generation facilities, water treatment and chemical plants and other sites that are critical components of our infrastructure. These sites bring with them some unique, more physical challenges than those in other markets. They often have a massive perimeter to protect. An airport, for example, could have a perimeter that's four or five miles, as opposed to the mere square footage of sites in other markets.

In addition to increased focus on the security of these sites, the critical infrastructure market is also undergoing substantial regulatory change. TSA mandates, TWIC, NERC, CFATS – these requirements demand a deep level of regulatory competency to ensure compliance. They necessitate customized security solutions that address the end-user's unique needs. And they require a higher level of funding and more sophisticated resources than ever before.” **SECURITY**

Don't Miss a Single Issue-Renew Now!
www.SecurityMagazine.com/2010