TRAFFIC MANAGEMENT SOLUTIONS
Enhanced video solutions improve situational awareness, resulting in increased traffic safety. p03

THE INTELLIGENT SECURITY OPERATIONS CENTER
A mission-critical control room should consider location, operator comfort, data convergence, and more. p04

TOWN EMPLOYS AXIS SURVEILLANCE
A Massachusetts police department installs a citywide surveillance solution that also addresses liability issues. p06

FIVE FEATURES OF AVIATION SECURITY
Airports are large, complex environments. Incorporating these steps will help streamline operations. p11

SELF-DRIVING VEHICLES
Autonomous vehicles may be ready for the road, but questions about safety remain. p08
Connecting the possibilities.

From concept to installation, to onsite training and annual service contracts, Vistacom creates Control Room solutions that support your critical mission.

For product info #51 securitymgmt.hotims.com

800-747-0459

www.vistacominc.com
THOUGHT LEADERSHIP: TRAFFIC MANAGEMENT

DATA-DRIVEN TRAFFIC MANAGEMENT SOLUTIONS

TECHNOLOGY COULD SAVE LIVES AND EASE CONGESTION.

By Stuart Rawling

IN 2016, there was just more than one death in the United States per 100 million vehicle miles traveled, according to the U.S. Department of Transportation’s National Highway Safety Administration. In 1980, the fatality rate was triple that. It’s hard to pinpoint precise explanations for the improvement, but safer cars, better driver education and awareness, and better traffic management all likely played a role in reducing road fatalities.

Yet modern transportation is hardly hunky dory. For starters, the major improvements in traffic accidents aren’t good enough. In the United States alone, more than 40,000 people lost their lives on the roads in 2017. In the European Union, more than 25,000 perished. In China, it is estimated that 700 people a day die in traffic accidents, amounting to more than 250,000 a year.

As road transportation safety has failed to improve, congestion has also gotten worse. Today, Americans spend the equivalent of an entire work week every year stuck in traffic, more than twice the amount of time that they lost to traffic jams in 1980.

Congestion isn’t just frustrating for drivers; it’s a major drain on the economy and it leads to increased air pollution, posing a threat to our health and the well-being of our ever-warming planet.

The solution to these problems lies in enhanced traffic management techniques.

Fortunately, an increasing number of cities around the world are embracing data-driven traffic management solutions to reduce congestion, accidents, and pollution.

The goal for new traffic management solutions is to provide traffic managers the clearest and most comprehensive view of the roads, bridges, tunnels, and intersections they oversee. Enhanced video camera technology, with multisensor panoramic cameras that provide a high-definition view of entire intersections with no gaps in coverage, is now part of that solution.

Intelligent analytics that help traffic managers identify a problem, even when personnel don’t see it in real-time on video, are becoming an essential piece of traffic safety and monitoring. For instance, one solution includes sensors that alert traffic managers to real-time issues that demand attention, notably when traffic flow has dropped below a certain threshold on a certain section of road or, more critically, if traffic has come to a complete stop. Other key issues that smart technology detects include vehicles moving in the wrong direction on the road or collisions. This automated incident detection capability becomes critical in tunnels where incidents can cause major delays.

That level of intelligence significantly reduces the amount of time and labor that it takes to recognize and react to a situation. The increasing sophistication of surveillance solutions helps emergency responders and public safety agencies keep much closer tabs on every part of the transportation system.

These technological advances must be designed to integrate with existing public agency workflows to maximize effectiveness. The interface to the video management system must be user-friendly and intuitive to surveillance industry veterans, as well as the increasing number of IT generalists who are being put in charge of surveillance operations. Ideally, the interface should display what’s needed, when it’s needed, allowing the user to easily switch between cameras while alerting the user to incidents that warrant attention.

The industry has the capabilities to enhance our quality of life and to save lives via improvement to traffic management solutions. Using the available technological solutions and analytics, it’s time to make a change.

STUART RAWLING IS DIRECTOR OF SEGMENT MARKETING AT PELCO BY SCHNEIDER ELECTRIC.
BUILDING THE CONTROL ROOM OF TOMORROW

CONSTRUCTING A MISSION-CRITICAL CONTROL ROOM ADVANCES THE ENTERPRISE.

By Dan Gundry

AT THE CENTER of an enterprise organization’s security operation stands its nucleus, arguably one of the most important pieces for overall functionality and efficiency: a command center or security operations center (SOC). A place where a variety of systems and solutions come together, the command center exists to provide a common operational picture, mitigate threats, and promote enhanced communication during an incident. The goal of any command center is to monitor, assess, and respond to a variety of threats and incidents. As technologies advance and trends develop, so too do the strategies in place to meet this goal. There are several considerations that must be made when designing the control room of the future.

Space. For many companies, a control room may be allotted space in a basement or small windowless room chosen as an afterthought. While some companies are limited by space, many decide the SOC's location is unimportant. This can be a big mistake when designing a control room that will serve the company now and into the future. It’s critical for this space to be large enough to house important equipment that allows operators to view the relevant incoming data and make informed decisions, but it’s also necessary for the space to be scalable as needs change, technology evolves and coverage increases, and a company grows.

Operator comfort. Space isn’t the only consideration when designing an SOC or control room. Central to the success of any organization is the ability for security operators to quickly and efficiently take information coming into an SOC and act on that information to identify risks and mitigate threats. Operator comfort, as a result, should be central to the design of a control room, taking lighting, console comfort, ergonomics, ambient noise, and temperature into careful consideration. If operators are uncomfortable or distracted, in pain with a sore neck due to bad viewing angles, or too warm in a room without proper ventilation, they can miss out on critical events or emergencies. Addressing these before they become problematic is crucial in the design stage of an SOC.

Technology. When it comes to building a mission-critical SOC, there’s a reason why large-scale video walls that showcase a number of incoming data points are dominant. Uniform and integrated visual elements are imperative to the success of an SOC or control room, because operators and first responders require the most up-to-date and complete information regarding incoming security-related events. Additionally, the technology needed to bring multiple data streams together in a single-pane-of-glass view is an important consideration to make, and hiring a control room integrator that specializes in this technology can streamline the process and result in better situational awareness across the board.

Data convergence. Command centers today combine a number of security components, but as end users demand an emphasis on the full umbrella of security rather than small silos, facilities are focused on including additional pieces, such as risk and threat assessment, employee travel, and social media monitoring. Data incorporation is also a critical element, and command centers must be able to collect any number of data points for effective data aggregation. Dashboards that can make sense of a large amount of information can streamline decision-making and response.

Innovation. While words like artificial intelligence and machine learning are often whispers around the industry, for innovative companies, these terms are becoming more commonplace as they enter a new frontier in how data is collected and analyzed to deliver information to security operators. The control room of the future brings innovative software and systems to the forefront, taking existing sensors that are providing a wealth of information and layering an additional method by which to understand what is happening and make decisions about the organization’s health.

Enterprise organizations rely on their SOC for business operations. In times of an emergency, and as risks become more severe, a complete situational picture is necessary. Taking into consideration the space, operator comfort, technology, data convergence, and future innovation can set security managers up for success in protecting their enterprises.

DAN GUNDRY IS DIRECTOR OF NATIONAL CONTROL ROOM SALES AT VISTACOM.
TOP FIVE CHALLENGES FOR MANAGING CYBERSECURITY RISK

TRUSTED IDENTITIES MAY PROVIDE PROTECTION AGAINST A RANGE OF THREATS.

By Pan Kamal

CYBERSECURITY THREATS continue to grow and evolve. Trusted identities combat these threats as part of holistic, end-to-end solutions that combine multifactor authentication, credential management, and physical identity and access management (PIAM) and are supported by real-time risk profiling technology plus digital certificates, all bringing trust to the Internet of Things (IoT). Following are five of the top cybersecurity risks where trusted identities provide critical protection:

1. Fighting fraud. Today’s risk management solutions use trusted identities and analytics to protect transaction systems and sensitive applications. Employing a combination of evidence-based capabilities, behavioral biometrics, and machine learning, these solutions help organizations detect phishing, malware, and fraudulent transactions. They can also prevent account takeovers and session stealing.

2. User experience and business decisions. Besides detecting threats, adding an analytics engine behind an organization’s archiving solutions, digital certificates, and user location information enables organizations to realize other valuable benefits. Predictive analytics help pinpoint threats and facilitate countermeasures by defining a user’s attributes and behavior so that risk can be assigned to people and areas. It also provides insights around personnel movement in a building so organizations can optimize workflows and the usage of facilities, common areas, and individual rooms.

3. Securing the IoT. Digital certificates add trust in the IoT and are becoming a core component for combating cybersecurity risks. Trusted cloud services are used to issue unique digital IDs to devices ranging from mobile phones, tablets, video cameras, and building automation systems to connected cars and medical equipment. One example is cloud-based secure issuance, in which the use of digital certificates creates a trusted relationship between the cloud and all issuance consoles, printers, and encoders. Industrial IoT is another area that is seeing huge adoption in critical industries like utilities, oil and gas, chemicals, pharmaceuticals, transportation, and more, being able to collect and correlate physical, IT, and operational events from IoT devices. This multidimensional information can provide indicators of compromise that are otherwise hard to detect with traditional means.

4. Plugging gaps in security defenses. The move to unified identity management reduces risk by extending multifactor authentication across an entire identity and access management lifecycle. A cloud-based model is used to provision IDs and perform authentication for physical and logical access control. The next step is to migrate to convergence solutions that pull everything related to identity management into a unified system capable of granting and managing access rights. PIAM software is a key element, unifying identity lifecycle management by connecting the enterprise’s multiple and disparate physical and IT security systems to other parts of the IT ecosystem, such as user directories and HR systems, as well as cloud-based card issuance systems, wireless locks, and location-based services.

5. Minimizing risks associated with GDPR compliance. PIAM software also simplifies General Data Protection Regulation (GDPR) compliance for physical security departments, automating previously manual processes of ensuring and documenting that all requirements are being met and data breach notification guidelines are being correctly implemented. It centralizes and applies policy- and rules-based automation for all compliance processes, from identity enrollment through auditing. It also ensures no individual names or other details are transmitted to access control systems, simplifies user consent procedures related to personal information, applies deep system integration to identify threat patterns, and provides robust compliance reporting.

PAN KAMAL IS VICE PRESIDENT, PRODUCT AND SEGMENT MARKETING AT IAM SOLUTIONS WITH HID GLOBAL.
LOCATED 30 MINUTES north of Boston, Massachusetts, the Town of Billerica strives to offer residents and visitors a safe, welcoming environment. To this end, the town’s surveillance system has been expanded to a variety of locations, including the town hall building, library, recreation areas, and apparatus bays of the fire department.

The surveillance cameras were originally installed for two primary purposes: as a deterrent and as a reactive tool for the Billerica Police Department (BPD). For example, given that one of the recreation areas often transforms into a gathering spot for kids and families, visible cameras on-site give a simple reminder that BPD will not tolerate illegal activity on the grounds. With a skate park, basketball courts, and a playground, cameras provide a way to deter general problems such as drug activity and vandalism.

WORLD-CLASS SECURITY, SMALL-TOWN FEEL

By Steve Stanberry, PSP
However, the town’s analog cameras became outdated. Recently, BPD decided to upgrade to an IP camera system for more effective and proactive security measures and clearer video.

Because the local school department had Axis IP products installed, BPD paid the administrators a visit to learn more. “When we went to upgrade our system, they recommended the Axis products,” says Greg Katz, lieutenant and accreditation and technology manager with BPD.

BPD turned to Axis network cameras to integrate physical access control and sound analytics. The solution also gives officers an intelligent surveillance solution to keep the peace and improve responses as incidents happen.

At the park, Axis P33 Network Camera Series have proven effective for the various recreational areas. The exterior models function in a variety of weather and temperature conditions. With the Axis Lightfinder technology deployed on the cameras, Katz says it is notably easier for officers to quickly address incidents and retrieve video. The tool provides clear, full-color footage at night when loitering and violations tend to occur.

Though BPD does not monitor the video feeds in real time, it uses surveillance reactively by responding to system-activated alerts or retrieving evidence for investigations. To process the footage, the town utilizes Axis Camera Station video management software.

In the case of a man causing a disturbance at the skate park one night, officers were able to go back to the video, which caught the whole incident, and apprehend the suspect. “Axis Camera Station has been working well for us,” Katz notes. “We use the mobile app as well. It’s all very functional for what we need.”

These installations were just the initial phase of deployments in Billerica, followed by a major project that outfitted the department’s building with a new, completely IP-based solution. Axis P3365-V Network Cameras were placed in the department’s lobby and stairwells. Two Axis Q3709-PVE cameras were mounted on each side of the building to grab a full 180-degree view at 4K resolution for detailed coverage over a wide area. Axis Q8414-LVS cameras were included in and around the holding cells.

Additionally, Katz and his team replaced an access control system with Axis A1001 Network Door Controllers at both the BPD station and the town hall. Controlled through settings on Axis Entry Manager, BPD has an updated door security solution that Katz says has been both reliable and easy to use.

As with other law enforcement agencies, BPD faces a great deal of liability for individuals held in custody. “We’re responsible for the well-being of those people,” Katz explains. “It’s our duty to supervise them and make sure they don’t hurt themselves.”

The department found opportunities to better keep watch over these individuals with physical access control and Axis Sound Intelligence’s Aggression Detector.

The station has policies in place to have personnel monitor the individual in the holding cell every 15 minutes. To quickly provide a log of these wellness checks, Katz pulls a report from Axis Entry Management. The station has policies in place to have personnel monitor the individual in the holding cell every 15 minutes. To quickly provide a log of these wellness checks, Katz pulls a report from Axis Entry Management.

“WE’RE RESPONSIBLE FOR THE WELL-BEING OF THOSE PEOPLE. IT’S OUR DUTY TO SUPERVISE THEM AND MAKE SURE THEY DON’T HURT THEMSELVES.”

AS WITH OTHER LAW ENFORCEMENT AGENCIES, BPD FACES A GREAT DEAL OF LIABILITY FOR INDIVIDUALS HELD IN CUSTODY. “WE’RE RESPONSIBLE FOR THE WELL-BEING OF THOSE PEOPLE,” KATZ EXPLAINS. “IT’S OUR DUTY TO SUPERVISE THEM AND MAKE SURE THEY DON’T HURT THEMSELVES.”

Katz adds that incorporating Sound Intelligence into the existing solutions is cost-effective. He says he plans next to install an Axis C2005 Network Speaker in the station’s dispatch center. With this tool, when the analytic picks up aggression, it can trigger an audio alert, such as a message that says, “Disturbance in cellblock number two. Please check.”

BPD foresees opportunity with sound analytics to secure other parts of the town, especially schools and recreational areas. These areas are typically dark and quiet at night and prone to vandalism, graffiti, and illegal activity that often goes unnoticed until the damage is done.

“We definitely see possibilities in the near future,” Katz notes. “The good thing about sound analytics is that they alert you when something comes up, giving you the opportunity to respond while it’s happening.”

BPD also intends to investigate how sound analytics can be augmented with motion-detection applications and the new radar technology from Axis.

“Every police officer wants to catch criminals in the act, not take a report after the fact” Katz says. “We want officers to be proactive, know when something is going on, respond, and address the situation before any damage might happen.”

STEVE STANBERRY, PSP, IS BUSINESS AREA DIRECTOR, NORTHEAST, FOR AXIS COMMUNICATIONS, INC.
To some, driverless cars are the stuff of nightmares and horror movies. Just the idea of riding in a fast and potentially destructive machine with no agency over speed and direction can feel disturbing on a primal level, like a living metaphor for being completely out of control.

It’s not surprising, then, that 42 percent of respondents in a recent survey said that they would refuse to ride in a self-driving vehicle (SDV). The survey also went a bit further: What if the driverless car had a stellar safety record? Nonetheless, 38 percent of respondents said they would not ride in one, regardless of its safety rating.
**THIS LEVEL OF SAFETY MAY BE NOT ENOUGH FOR MOST PEOPLE TO GIVE UP THEIR CONTROL OF VEHICLES AND ENTRUST THEIR LIVES TO SDVS.**

Conducted by J.D. Power, the results of the survey of 1,000 U.S. respondents was released in early October at the Auto Summit, an event held by the University of Michigan Transportation Research Institute. It also found that a slightly larger group of respondents, 45 percent, would ride in an SDV if it were 100 percent safe, with a zero error rate.

But even if a 100 percent safety rate were achievable, finding an institution that most people would trust to issue a safety rating could be a problem, the survey found. Only 12 percent of respondents said they would trust the manufacturers to test SDVs for safety, and just 9 percent said they would trust the government. The Insurance Institute for Highway Safety gained the trust of 29 percent of respondents, making it the most trusted testing body. But the highest number of respondents, 40 percent, said there was no organization they would trust to conduct safety testing on SDVs.

And these types of concerns about SDVs are not merely an American phenomenon, but they are prevalent in countries around the world, experts say. For example, in China, researchers Peng Liu and Run Yang of Tianjin University, and Zhigang Xu of Chang’an University, realizing that safety remains a big issue with SDVs, decided to examine the following questions: When it comes to SDVs, how safe is safe enough? What is the socially acceptable risk level?

The study found that respondents believe SDVs should be four to five times as safe as conventional cars. So, using the current global traffic fatality risk of an estimated at 17.4 fatalities per 100,000 drivers, the acceptable global fatality risk of SDVs would be about three to five fatalities per 100,000, according to the study’s findings, which were published earlier this year in the journal *Risk Analysis*.

This four-to-five-times safer standard surprised Liu, who is an assistant professor in the department of industrial engineering at Tianjin University. “Certain regulators suggest that if SDVs are twice as safe as the average human driver, we should consider allowing them to operate on public roads,” he told Security Technology in a recent interview. “And it is definitely great technical progress if the safety of SDVs reaches this level. However, our finding suggests that this level of safety may be not enough for most people to give up their control of vehicles and entrust their lives to SDVs.”

Moreover, it seems entirely possible that this highly desired safety standard is not widely understood in the government and industry communities, he adds. “Policy makers, regulators, and the transportation industry seem to not pay sufficient attention to the need and voice of the public in terms of the safety of SDVs,” Liu says. “An effective public discourse among many stakeholders is necessary to arrive at a consensus about the acceptable safety of SDVs.”

To contribute to this discourse, the researchers proposed risk level requirements for SDVs that divide risks by three categories: unacceptable, tolerable, and broadly acceptable.

Under this proposal, SDVs that are less safe than conventional cars would be in the unacceptable risk category. In the tolerable risk category are SDVs that are four to five times as safe as human drivers. The broadly acceptable risk category would be set as two orders of magnitude lower than current global traffic risk, or about 0.17 fatalities per 100,000. That broadly acceptable risk level is somewhat similar to the risk level of public transportation modes such as rail and commercial aviation.

But concerns about safety levels aside, the U.S. government is rolling forward with its own proposals for encouraging the development of SDVs. In October, the U.S. Department of Transportation (DOT) released *Automated Vehicles 3.0: Preparing for the Future of Transportation*, a strategic plan and set of guiding principles for a policy framework that will encourage the development of SDVs.

The new plan sets out six guiding policy principles from DOT moving forward: prioritizing safety; remaining technology-neutral, so the public can choose the best technologies instead of what government dictates; modernizing or eliminating regulations that impede the development of SDVs; encouraging a consistent regulatory environment free of state-by-state conflicts; preparing proactively for automation with pilot programs and best practice guidance; and protecting the rights of citizens to choose conventional cars instead of SDVs.

The plan also acknowledges current safety and security concerns, and DOT pledges to prod the private sector to develop solutions to secure SDVs from hacking and other threats.

“...the public has legitimate concerns about the safety, security, and privacy of automated technology,” U.S. Transportation Secretary Elaine Chao said in the plan’s introduction. “So, I have challenged Silicon Valley and other innovators to step up and help address these concerns.”

**MARK TARALLO IS SENIOR EDITOR AT SECURITY MANAGEMENT.**
SECURING COMPLEX AVIATION ENVIRONMENTS

FIVE STEPS TO HELP STREAMLINE SECURITY OPERATIONS.

By Mark Folmer, CPP

SECURITY LEADERS in complex environments like airports deal with a large number of players, roles, responsibilities, and technology. Following are some challenges aviation security leadership faces, and the systematic solutions that can be employed to help overcome them.

Moving parts. The sheer volume of moving items, versus typically static ones, in airports can be overwhelming for security professionals. For example, in U.S. airports security leaders must on an average day contend with 2,100 flights from other countries, and 325,000 passengers from approximately 280 airports, according to the U.S. Department of Homeland Security. These passengers, their luggage, and personal electronic devices need to be screened.

Multiple players. Both in the United States and Canada, the law requires a law enforcement presence at airports. These officers may be under private, local, state/provincial, or federal jurisdiction.

As a mix of public, commercial, and passenger spaces, the airport must balance delivering a welcoming environment for passengers while maintaining stringent security standards. Different security companies may be involved in this balancing act.

Technology. Layers of technology that help mitigate security risks in airports must be added to the equation: license plate recognition, facial recognition, biometrics, x-ray security screening, access control, surveillance, and more, with each device feeding data to people or other devices.

Big Picture. From an enterprise security risk management perspective (ESRM), properly managing security risk means risk must be looked at across an entire enterprise, irrespective of departments or stakeholders. Because threats today can come from physical and IT access points, convergence is intertwined with ESRM.

The stakes rise rapidly during an incident, when the players need to work together to ensure coordinated response. With this many stakeholders distributed over so much territory, how can you get the diverse players speaking to each other in the same language?

SOLUTIONS

The following five features should be present in solutions that solve the challenge of information sharing and interdependence among multiple stakeholders in aviation environments.

1. Data. Unlike Esperanto, the constructed human language that aimed to become a medium for international communication, there is a common language that can successfully unite all security stakeholders—data. Data breaks down barriers of communication and does it in real time.

2. Analytics. The right software can identify incident trends so the stakeholders can better mitigate and manage risk. With improved focus on areas of vulnerability, stakeholders can assign resources efficiently and reduce incidents.

3. Notifications. The system solution must provide real-time visibility into the location of security assets and what they are doing. As a result, leaders stay on top of all resources, and commitments to other stakeholders can be fulfilled.

4. Process documentation. The system solution should make it easy for a guard to comply with established protocols, service level agreements, and stakeholder requests. It should also enable leadership to access, review, and analyze historical security data to support better security decisions moving forward.

5. Cost effectiveness. Security is often seen as a cost. But the right security solution will give you the tools to identify trends and streamline operations so you can run your organization more efficiently. The right solution will deliver insight into key profitability indicators and help you focus on quality service.

MARK FOLMER, CPP, IS VICE PRESIDENT, SECURITY INDUSTRY AT TRACKTIK.

December 2018 Security Technology 11
A few years ago, Titan Security Group, a security services provider based in Chicago, Illinois, was looking for better technology that would help the company maintain a competitive advantage in the bustling Chicago market. They had scheduling software to help coordinate officers in the field, but that didn’t give senior leadership the kind of enterprise-level management capabilities they were looking for. That’s what led them to TEAM Software in 2015.

“We had been using another solution with no integration to financials,” said Dave Pack, who has been the Executive Vice President of Titan Security for the past eight years. “It was basically a scheduling package, and it had nowhere near the level of detail or reporting capabilities that TEAM has.”

That level of detail comes from a holistic business management software system with the core solution, WinTeam, as its backbone. All financial, operations and workforce management data is shared throughout the system to streamline business processes, build efficiency and give insight into profitability down to the job-site level. Pack points to that shared data as a big benefit for the business in terms of building financial awareness and eliminating silos of information.

“With the benefit of the integrated operational and financial data, we can put the right information into our operators’ hands,” Pack said. “We can have a dialogue about expectations and results on the job level, and share that information and data with our clients. It helps increase transparency and provides a sense of ownership.”

Pack explained that the company’s main objective is to bring as many business processes and as much data as they can into the system. In fact, Pack noted that the company plans to use the work ticketing component of WinTeam, typically used by commercial cleaning firms, for the company’s electronics division.

Pack also noted that using TEAM’s trusted solutions helps them recruit top-level talent.

 “[TEAM’s] products have a great reputation in the security industry. That reputation helps us attract and recruit the best operators in the Chicago marketplace. Titan’s diverse senior management is comprised of the best-of-the-best in the industry and they expect to have a system with TEAM’s reputation and functionality,” Pack said. “Our newest VP of Operations says there is no excuse for lack of success with all the information available from this system.”

Leveraging an industry-specific, all-in-one platform has supported the company’s success competing to win new business and serving customers, as well. Titan schedules approximately 54,500 hours per week and employs more than 1,600 security staff.

“The technology has definitely allowed us to scale more effectively. A lot of our national competitors struggle in Chicago because it is a very unique, customer-focused market,” Pack said. “Each building is unique, so to be able to report operational data, financials and invoices in different ways is important to our clients. Our ability to bill in multiple formats allows us to never say no to clients or prospects. We provide high-touch customer service, so we want to say yes.

“In the Chicago market, there is a lot of activity and opportunities for Titan,” Pack continued. “We have very professional operators, and with a system like TEAM and all of its bells and whistles behind us, we can compete with anybody.”

TEAM SOFTWARE DEVELOPS SOFTWARE FOR SECURITY CONTRACTORS OF ANY SIZE. THE WINTEAM ERP IS PERFECT FOR MEDIUM TO LARGE SECURITY ENTERPRISES, LIKE TITAN SECURITY GROUP, WHO NEED A HOLISTIC SYSTEM THAT HANDLES FINANCIALS, SCHEDULING AND OTHER OPERATIONS FUNCTIONS AND THAT CONNECTS THE BACK OFFICE TO THE FIELD. NEW IN BETA, TEAM IS PROUD TO INTRODUCE Q BY TEAM SOFTWARE, A RIGHT-SIZED SOLUTION FOR SMALL SECURITY CONTRACTORS WITH 100 EMPLOYEES OR FEWER WHO NEED VISIBILITY INTO THE FIELD AND TIME-SAVING FEATURES.

For product info #52 securmgmt.hotims.com