KICKING OFF THE CEREMONY was the Southwest DeKalb High School Band, followed by comedian Scott Bloom, the master of ceremonies, who welcomed attendees of both the Seminar and Exhibits and those of the (ISC)² 4th Annual Security Congress. Bloom intermingled jokes with highlights of the rich history of ASIS. He also welcomed familiar faces within the association to the stage to share the origins of ASIS. Former ASIS President Don Walker, CPP, was one of many who made a surprise appearance at the ceremony, taking a moment to give an overview of the history of the event, which began in 1955.

ASIS International’s 60th Annual Seminar and Exhibits began bright and early Monday morning, with marching band fanfare and special appearances by former ASIS presidents. “For the past 60 years, our Seminar and Exhibits has been in the forefront of security’s advancement by supplying the ultimate venue for the exchange of visionary technologies, ideas, and solutions—all designed to raise the knowledge, professionalism, recognition, and respect of the security practitioner,” said ASIS President Richard Widup, Jr., CPP. All of this comes together to enable ASIS Seminar and Exhibits attendees to “Succeed Today by Seeing Tomorrow,” which was the event’s theme.
Colin Powell spoke at Wednesday’s General Session.

That first year, the seminar was held at the Sheraton Carlton Hotel in Washington, D.C., with 100 attendees. Members paid $5 to register and the event made a profit of $9.25. One year later, in 1956, 11 exhibitors showcased their products and services. President Dwight D. Eisenhower also honored the event with the gift of a telegraph, symbolically expressing the importance of the association’s role in securing America.

Sixty years later, ASIS has become a global association with a focus on international security education. In one of the many video segments of the ceremony, Widup said that the biggest challenge for new members and first-time attendees is often “trying to decide how many sessions they can squeeze in” during the four-day event.

Some of the options these attendees have to choose from include six general sessions, 185 educational sessions, four networking lunches, three keynote speakers, exhibitors, and CSO Roundtable events. “This, including the myriad of networking opportunities, makes for a busy and productive event,” Widup added.

The Seminar and Exhibits has also increased its international presence, with more than 200 security practitioners from Nigeria in attendance this year, for example, and an overall increase of 30 percent more international attendees during the past 10 years. Additionally, the exhibits have grown to occupy 607,000 square-feet.

Widup invited the ASIS Board of Directors on stage to cut the ceremonial ribbon, signifying the opening of the exhibit hall.

### Special Sessions

**The ASIS International 60th Annual Seminar and Exhibits** in Atlanta was the scene for keynote addresses by two of the most influential men in the United States during the last decade—former Utah Governor and Ambassador to China and Singapore Jon M. Huntsman, Jr., and former Secretary of State General Colin Powell (U.S. Army-ret.)

#### Huntsman

On Tuesday morning, Huntsman described the rise of China and its implications for the United States.

Huntsman said that key to China’s future is the emergence of Xi Jinping, the current president of China. Xi’s father, a communist party veteran, was imprisoned during the Cultural Revolution, and so Xi knows the machinations of Chinese politics on a personal level.

Xi also seems to understand the massive amount of change needed to keep China’s economy developing, as China’s state-owned enterprises need to be reformed and Chinese consumers need to be persuaded to spend more. In turn, China’s spending and consumption will drive the economic relationship between China and the United States in two significant ways. First, it will result in a larger market for U.S. exports to China.

“They’ll create more of a consumption generation [who] will want to buy more of American products,” he said.

Second, China’s economic growth will also result in more Chinese investment in the United States, something that will benefit states and localities. “I can’t think of a governor or a mayor in this country who wouldn’t want to say, ‘Bring it on,’” Huntsman said.

These economic ties will have a stabilizing effect on the U.S.-China relationship. Conflicts will inevitably occur, such as disputes over Chinese hackers targeting the United States, but leaders of both
countries will not want to lose the economic benefits.

“We’ll have challenges, and we will seemingly be at the breaking point at times, but the underlying reality will be that the relationship is too big to fail,” Huntsman said.

Huntsman has been a prominent figure in American politics and diplomacy for more than a decade. After serving as U.S. Ambassador to Singapore in the early 1990s, he was elected as governor of Utah in 2005. In 2009, the Obama administration appointed him as U.S. Ambassador to China. In 2011, Huntsman resigned and later that year declared his candidacy for the 2012 presidential election, but the campaign never gained traction.

Given his independent streak, Huntsman seems a natural fit for his current position as cochair of No Labels, which describes itself as a national movement of Democrats, Republicans, and independents dedicated to problem solving. The group plans to build a national strategic agenda, with four policy goals: create 25 million new jobs over the next 10 years; secure Medicare and Social Security for the next 75 years; balance the federal budget by 2030; make America energy secure by 2024. The group plans to release its national agenda, then advocate for it during the next presidential election. “Nobody’s talking about this stuff that really matters,” Huntsman said.

While some have suggested that the agenda could form the basis for a third political party, Huntsman said that his No Labels group recognizes that the United States will keep the two-party system for the immediate future. “It’s going to take Republicans and Democrats to get us out of the hole,” he said. But things will change in the long-term, he added.

POWELL

It was a full house in the Georgia World Congress Center when former Secretary of State Colin Powell took the stage for Wednesday’s keynote address. Powell entertained the audience with anecdotes from his personal life since retiring from the political arena. “At this stage in my life, I’m just happy to be anywhere,” he quipped, but added, “I’m probably as busy now as I’ve ever been.”

Powell’s speech took a more serious tone as he dove into the issues facing the United States and the security industry today. He explained that while security is crucial, it shouldn’t be taken to a point where the growth of American society is hindered. “We have to make sure that we don’t secure ourselves so well that we’re not getting the work done, we’re not doing what we need to do,” he said. “We have to make sure we have the right balance.”

Powell told the crowd that security professionals have the responsibility of making the country safe but welcoming. “Everything is now vulnerable, and so what responsibility you all have is to make sure that you protect people, protect institutions, protect our seniors, but at the same time do it in a way...that’s increasingly transparent so that people can’t even see that they’re being protected in the best possible way,” he said. “And I congratulate you for the work you’re going to be doing.”

Powell also touched on the ubiquity of threats that exist due to the digital revolution, which he has seen rapidly expand during his public service career. While the availability of smart devices has made the world a wider place, where it’s easier to share information, “within that open world there are incredible vulnerabilities that you have to deal with,” he said.

He received applause when he candidly expressed his frustration with the lack of progress on Capitol Hill. “In all my years in government...I have never quite seen it like this, seen it absolutely locked up and constipated where they can’t get anything done.”

Powell said he’s now focusing on young people, hoping to foster leadership in a new generation. Recently, he founded the Colin Powell School for Civic and Global Leadership at the City College of New York in Harlem.

For more on the Huntsman and Powell keynotes, see Security Management’s December issue.

Jon Huntsman, Jr., was the keynote speaker on Tuesday.
President’s Reception
Swimming with the Fishes

Like a school of hungry minnows, seminar attendees made their way to the Georgia Aquarium Monday night for the ASIS International Annual President’s Reception, where they networked, ate food and drink catered by Wolfgang Puck, listened to live music, and marveled at countless varieties of exotic fish and other unusual aquatic species.

The popularity of the event was clear right from the 7 p.m. start, as the line to enter the aquarium stretched roughly a quarter mile outside the venue. Once inside, attendees were given full access to the aquarium’s maze-like passageways, featuring row after row of water tanks and other animal habitats. Particularly popular among attendees were the beluga whales, albino alligators, red piranhas, and the African cichlids, an exotic fish found in Lake Malawi in East Africa.

“ABSOLUTELY BEAUTIFUL” is the way one new ASIS member and first-time attendee, Juliet Anabor, described the colorful surroundings.

In the ballroom, a funk band jammed while attendees ate and chatted. Video footage was projected on several walls, mainly of fish and animals but also featuring at least one human: Richard E. Widup, Jr., CPP, who was filmed in scuba gear, waving before putting on his mask and submerging in the aquarium’s main tank. A diver who may—or may not—have been the Society’s president was then seen swimming underwater holding a sign that read “Welcome to the ASIS President’s Reception, sponsored by AlliedBarton.”

Was it Widup? “However you want to frame it,” laughed ASIS CEO Michael J. Stack.

Reception attendees came from all over the world, and for different reasons. For Anabor, who is a judge in Lagos, Nigeria, the main attraction of the Seminar and Ex-
hibits was the exhibit floor. The court for which she works has a growing interest in industrial security. “We want to improve on our access control,” she said.

In contrast, longtime ASIS member Wilson O. Esangbedo, CPP, executive secretary of the Nigerian Institute for Industrial Security, said he has attended more than a dozen Seminars and Exhibits. Esangbedo said the professional networking is his favorite aspect of the event.

In particular, he was looking forward to the “Nigerian Night” networking event on Wednesday evening, an annual occurrence that sometimes draws more than 800 ASIS members from Africa. Besides networking, the education sessions are also a key reason for his attendance, he added.

Himmat Singh, managing partner with Maximus Capital Partners, said he was looking forward to hearing Jon Huntsman, Jr.’s Tuesday keynote speech. Singh said Huntsman was one of his heroes.

The Seminar and Exhibits was Singh’s first. He said he decided to attend because his firm was taking a greater interest in security.

Martin Barye-Garcia, security director in Latin America for Mars Incorporated and a member of the ASIS CSO Roundtable, said he was particularly impressed with a Monday morning CSO Roundtable session featuring Tom Ridge, former U.S. homeland security director and governor of Pennsylvania, who chairs the U.S. Chamber of Commerce’s National Security Task Force.

Ridge indicated that he understood the importance of government-industry cooperation when it came to U.S. security, and respects the contributions of security leaders. “He knows what our roles are as CSOs,” Barye-Garcia said.

And Stack, assessing the Seminar and Exhibits thus far, said he was encouraged by positive signs such as a standing-room-only crowd for Monday’s opening session, positive feedback on the speakers, and a full exhibit hall floor. “That’s a good thing,” he said.

EXHIBITORS WHO WISHED to compete for an Accolades Award submitted products and services introduced within the past year to a team of judges who evaluated the entries. The judges represented end users as well as experts in physical and information security. Companies were asked to describe a problem with existing security technologies, or a security problem area with no real solutions previously available, then explain how their new product or service solved the problem or filled the void.

The winners are:

**NICE SYSTEMS**

**NICE Suspect Search**

NICE Suspect Search is a patent-pending, video analytics-based technology that efficiently and quickly helps locate and track a specific person, reducing search time from hours to minutes. Users can track a target individual’s movements and access all relevant video recordings.

**QUANTUM TECHNOLOGY SCIENCES, INC.**

**Quantum Remote Intrusion Detection System**

Quantum Remote is a security solution capable of using a single concealed ground sensor to maintain an awareness perimeter. Potential threats on land, underground, in the air, and in the water are detected, tracked, and classified in real time.

**SENSTAR INC.**

**CyberVigil Security Switch**

Honorable Mention

CyberVigil is an industrial cybersecurity Ethernet switch that provides unique protection for physical security and industrial control systems against cyberattacks. It features full networking capabilities.
and is optimal for physical security networks, SCADA systems, and utility control networks.

**RoboGuard: Outdoor Perimeter Security**
RoboGuard is an agile robot, traveling on a monorail along smart fences. It carries an assortment of payloads such as a fence scanner, cameras, and intercom. It can replace manned patrols and can provide a first response to intrusion alerts.

**SENTRY360**
SentryEdge NVR Server Switch
SentryEdge is an ecosystem-driven appliance that combines a server and smart network switch. It allows flexible video-management software options and versatile storage selection such as NAS, RAID, and third-party storage systems.

**TYCO SECURITY PRODUCTS/CEM**

**CEM Emerald**
With its sleek design and state-of-the-art LCD touch screen, CEM Emerald offers card reader and controller functionality, fully integrated Voice-over-IP intercom, and a range of server-based applications.

**TYDENBROOKS**

**Krateus from TydenBrooks**
*People’s Choice Award*
Krateus from TydenBrooks, powered by LoJack SCI, is a reusable, rechargeable security device that tracks and monitors an entire shipment, down to the individual package. The product measures temperature, breakage, route deviation, radiation, pallet separation, and more. The device is powered by LoJack SCI, a leader in supply chain/cargo monitoring and security.

**VESDA-E Series Aspirating Smoke Detector**
VESDA-E is a smoke detection system with increased longevity, improved dust rejection, and greater area coverage, while allowing convenient detector mounting for ease of service and maintenance.

Congratulations to all winners and thanks to all entrants. ASIS looks forward to seeing the industry’s best at next year’s exhibits in Anaheim, California. ✨

**Experience Is Everything**

The ASIS International Young Professionals (YP) Group, in partnership with its exclusive sponsor, Securitas Security Services USA, is pleased to announce the winners of the 2014 Seminar Experience:

- **Jean-Charles Gris** (Montreal Chapter)
- **Kara M. Monroe** (Central New York Chapter)
- **Angela J. Osborne** (Abu Dhabi Chapter)

Nearly 50 entries were received and evaluated by a panel of ASIS member judges. Each winner received four nights of free lodging, complimentary ASIS 60th Annual Seminar and Exhibits registration, tickets to attend the President’s Reception and Foundation Night, and a travel voucher worth up to $500.

“This is the first time I will attend the ASIS Annual Seminar and Exhibits,” said winner Jean-Charles Gris in Atlanta. “My ASIS membership and leadership within the Montreal Chapter have significantly contributed to my professional growth and I am certain this event will be a flagship experience in my development.”

ASIS young professional Toby Heath, CPP, PSP, who managed the competition, notes, “This investment clearly illustrates that both Securitas and ASIS care about the future of the security industry.”

“The critical role of the security management professional in business has come into sharp focus in the years since 9-11. As such, the profession is drawing increased interest from both college-bound students and those seeking a second career,” observes ASIS President Richard E. Widup, Jr., CPP. “To meet the unique education and career development needs of young professionals within the security industry, ASIS founded the YP group in 2010. We are indebted to Securitas for its commitment to the next generation of security management professionals and for its generosity in partnering to establish the Seminar Experience.”
“The ASIS Seminar and Exhibits provides an unmatched opportunity for YPs to gain a better understanding about their fields of interest, learn about state-of-the-art technology, and network with their peers who represent the entire spectrum of security knowledge, skills and abilities,” notes Don Walker, CPP, chairman of Securitas Security Services USA, Inc. “Securitas USA is proud to make this unique opportunity available to three young professionals who otherwise may not have been able to attend the ASIS Seminar in Atlanta this year.”

More on the ASIS Young Professionals can be found at www.asisonline.org. ♦

**ASIS Councils at the Ready**

**quick glance** through the sessions scheduled during the ASIS International 60th Annual Seminar and Exhibits made it clear that many were sponsored by an ASIS council. Continuing education about the latest topics in security has always been a primary responsibility of the councils, and current council members worked for months crafting topics and recruiting speakers.

WHEN NOT FOCUSING on seminar sessions, members of the various ASIS councils were available to meet with prospective members to discuss their specialty area of security at council booths.

The Information Technology Security Council shared the latest edition of its newsletter. Two councils, Crisis Management and Business Continuity and Investigations, had brochures on hand that explain their programs and objectives.

The Leadership and Management Practices Council had copies of policies, guides, and articles on mentoring leaders and security metrics. The Law Enforcement Liaison Council pointed interested attendees to *Operation Partnership: Primer on Getting Started*, a how-to booklet on developing public-private partnerships. Other councils had audiovisual presentations that ran continuously at their booths.

**SHARE A MEAL**

Attendees could also express their interest in a specific council by engaging with its members during the Networking Luncheons on Monday, Tuesday, and Wednesday. Council members were seated at designated tables in the luncheon room.

No matter what industry or what aspect of security, members of ASIS councils were ready to give attendees the facts needed to perform smartly in their daily assignments and think strategically about their future in security. And best of all, new council recruits were welcome. ♦
Kicking off the night’s networking events was the Young Professionals (YP) Reception. Membership with the Young Professionals Group is offered to ASIS members below the age of 40, or those who are young in their career, with less than five years in the security industry. Toby Heath, CPP, PSP, YP co-chair, said he hoped that the conference would offer an opportunity to highlight mentorship. “I hope to continue to raise the awareness about the communication gap between young professionals in the industry and mentors,” he stated.

At the YP Reception was Wanda Lothrop, security coordinator for General Atomics in San Diego, California. She also serves as secretary of the local ASIS chapter, which paid her way to the Seminar and Exhibits. “It gets you out of your bubble, and you realize just how big the security industry is,” she noted.

Wanda Lothrop, security coordinator for General Atomics in San Diego, California, at the YP Reception.

NEWBIES
At the First-Time Attendee/New Members Reception, ASIS President Richard E. Widup, Jr., CPP, remarked that 60 years of ASIS Seminars and Exhibits would not have been possible without the many volunteer leaders who gave both time and effort to make the event a success. He asked the volunteer leadership who were present to raise their hands to identify themselves then told attendees, “Feel comfortable walking up to any one of these folks and saying, ‘I have an idea,’ or ‘I don’t understand this,’ because we’re all here to help make this event for you that much more enjoyable and pleasant, because we want to see you come back.”

Dennis Ramberg of Gothenberg, Sweden, a qualified risk and safety coordinator, received a scholarship from his country to attend the conference. “The security awareness in America is much greater than in Sweden,” he said, noting that he was looking forward to meeting security professionals from all over the world during the week.

WELCOME
Rounding out the night was the Welcome Reception, which was open to all attendees. Security professionals networked over cocktails and an array of hors d’oeuvres.

One attendee, Saleem Bukhari, corporate asset protection site supervisor at Ralph Lauren, was looking forward to the educational events. “I want to learn more about asset protection to advance my career,” he said.

A mixer was held at the ASIS International 60th Annual Seminar and Exhibits on Sunday night.

Mixer Mashup

An array of mixers, which offered something for every attendee, were held at the ASIS International 60th Annual Seminar and Exhibits on Sunday night.
On Monday, five ASIS International members who have held leadership positions in both signature and emerging ASIS initiatives were called on stage by ASIS President Richard E. Widup, Jr., CPP, to receive the prestigious President’s Awards of Merit.

Dr. Linda F. Florence, CPP, was honored for her volunteer service as a trustee of the ASIS Foundation. While Florence has held numerous volunteer leadership positions with ASIS through the years, this honor particularly recognizes Florence for her skilled leadership as the Foundation Board president.

A member of the Las Vegas Chapter, Florence is the vice president of SEE, Inc., in Las Vegas, Nevada.

Alfredo Iturriaga, CPP, was spotlighted for two significant contributions to the mission of ASIS. He is not only a member of the Professional Certification Board, but he has also contributed many hours of advice and counsel in preparing the Spanish translations of the certification reference materials and exams. A member of the Chile Chapter, Iturriaga is the executive vice president, RacoWind Consultores, Ltda, in Santiago, Chile.

Linda C. Harmon and Lisa Dolan, CPP, were recognized for their outstanding leadership in developing relevant content and networking opportunities for the ASIS Women in Security Group. As an example of their efforts, they contributed to a range of Seminar and Exhibits programming, including educational sessions, networking receptions, and joint ASIS and (ISC)² workshops. A member of the Phoenix Chapter, Harmon is the deputy director of global asset protection for Accenture in Phoenix, Arizona. Dolan is president of Securit in Flushing, New York, and a member of the New York City Chapter.

Bryn M. Palena was honored for her outstanding leadership of the ASIS Young Professionals Group. Through her efforts, the Seminar and Exhibits included relevant content and meaningful networking opportunities for the next generation of security leaders. A member of the Greater Philadelphia Chapter, Palena is an executive with First Advantage in Phoenixville, Pennsylvania.

Linda C. Harmon (left) and Lisa Dolan, CPP, receive their awards from ASIS President Richard E. Widup, CPP.
Widup also presented the Don Walker Award for Enterprise Security Executive Leadership. Given for superior advancement of security management education, this year the honor went to Per Lundkvist, CPP, PSP, PCI, security director and CSO of Crane Currency of Tumba, Sweden. “Per embodies the qualities this award was created to applaud. He is an individual who promotes and adopts security standards, provides ongoing support and encouragement of continuing education, encourages professional certification, and promotes the development of security leaders,” said Widup.

The winners of this year’s Accolades Awards were also bestowed. (See page 5 for all the winners.)

The luncheon was sponsored by VirSec, a Huffmaster Company.

TUESDAY
Widup announced the 2015 Board Management Committee of the ASIS International Board of Directors. (See page 17 of the regular issue).

Retiring from the chairmanship of the Board is Geoffrey T. Craighead, CPP, vice president of Universal Protection Service in Santa Ana, California. “There are few things I have done in my life that have given me as great a sense of satisfaction as working with such an impressive, wonderful, and dedicated group of volunteer leaders, as I have had the pleasure to meet during my years with ASIS,” Craighead said. “It has been my sincere privilege and honor serving ASIS all these years.”

Tuesday’s luncheon marked the last major function of Craighead’s voluntary service to the Society, but he said that he intends to remain involved and “heartily” committed to the “health, growth, and success of ASIS.”

Along with recognizing the volunteer leaders of ASIS, Widup also announced the winners of the Roy N. Bordes Council Member Award of Excellence. This award recognizes outstanding volunteer achievement and significant contribution to ASIS through council involvement. The 2014 award was given to James T. Roberts, Jr., CPP, president of Starboard Focus Continuity Planners.

Roberts has been a member of the ASIS Law Enforcement Liaison Council since 2001 and serves as the vice chair. He is also the chair of the ASIS Law Enforcement Liaison Council’s IACP Liaison Committee. Additionally, Roberts is a member of the ASIS Critical Infrastructure Working Group.

His award “specifically acknowledges and recognizes the work that is accomplished by a member who selflessly serves on councils, sharing experiences, and bringing the latest solutions to ASIS educational programs and publications,” Widup said.

Widup also presented the E.J. Criscuoli, Jr., CPP, Volunteer Leadership Award. “Today’s recipient joined ASIS International in 1981 and has been an active volunteer leader starting as a chapter chair in 1984.”

“His commitment to the advancement of the security professional and ASIS chapter development in California are inspiring. Secretary, treasurer, program chair, assistant regional vice president, and regional vice president are
just a few of the titles he has held, and all with distinction. I am truly honored to present to you the very well-deserving 2014 E. J. Criscuoli Jr., CPP, Volunteer Leadership Award recipient, Wayne K. Cartwright, CPP.”

Cartwright is principal consultant for Security Management Solutions of Tustin, California.

Widup also took a moment to recognize (ISC)², which is celebrating its 25th anniversary and the fourth year collocating its Security Congress with the Seminar and Exhibits.

“The combined conferences bring together operational and information security professionals to create the world’s most influential security event,” (ISC)² Executive Director Hord Tipton came to the stage to tell attendees. “Together, ASIS and (ISC)² are leveraging expertise and resources to present two events in the same location with an overarching goal: to provide information security and operational security professionals with the knowledge, technology, and networking opportunities they need to excel in their careers and secure their organizations’ people, property, and data.”

WEDNESDAY

ASIS Treasurer David C. Davis, CPP, welcomed special guests to Wednesday’s luncheon, which celebrated law enforcement and the military. “As a former member of the law enforcement community, I am honored to host today’s luncheon program and am keenly aware of the essential relationship that exists between the military establishment, law enforcement, first responders, the public sector as a whole, and ASIS International,” he said.

“Since its founding almost 60 years ago, ASIS has consistently fostered cooperation between our membership and the public sector communities. Today, cooperation is the key that unlocks the door to our mutual success locally, as well as around the world. Teamwork and cooperation are critical if we are to achieve our mutual goals and combat the forces that align against us,” noted Davis.

Members of the military and law enforcement officers were asked to rise and received the applause of the crowd. Davis told them, “Let’s remember that the base of our society is closely linked to these communities. Keeping in mind how many of our current members came to us through law enforcement and military careers, I now ask all former members of public-sector law enforcement—be they U.S. or non-U.S., federal, state, or local—and of all branches of the U.S. and non-U.S. military to please rise and be recognized.”

Dan Waddell, director of government affairs, (ISC)², addressed the guests and attendees, saying, “It is important for all of us to remember that there are several people behind the scenes—from a military, law enforcement, and first responder perspective—helping to keep both the lines of communication and our forward locations open and secure during disasters—whether caused by natural forces or through heinous acts of terrorism. This is a great example of the importance of understanding both logical and physical security…and the reason why we’re here this week.”

Among the special guests at the head table were Chief Connie Sampson, Georgia State University Police; U.S. Marshal Beverly Harvard, Northern District of Georgia; Special Agent in Charge Ray Moore, U.S. Secret Service; Chief Cassandra Jones, Fulton County Police; Chief George N. Turner, Atlanta Police Department; and

**Security Book of the Year**

ASIS International presented the inaugural Security Book of the Year Award on Monday in the ASIS Bookstore at the 60th Annual Seminar and Exhibits. Michael J. Fagel, Ph.D, received the award for *Crisis Management and Emergency Planning*. The book supplies time-tested insights to help communities and organizations be better prepared to cope with natural and man-made disasters. The author presents advanced emergency management and response concepts not often covered in other publications.

Fagel’s professional career spans nearly four decades in fire, rescue, emergency medical services, law enforcement, public health, and emergency management, as well as corporate safety and security. Currently, he is an instructor at the Illinois Institute of Technology—Stuart School of Business’s master’s in public affairs program, as well as at Northwestern University in the master’s program in public policy and administration.

Fagel spent 10 years at the U.S. Federal Emergency Management Agency in the agency’s occupational safety and health cadre, responding to incidents and disasters such as the Oklahoma City bombing.
MOORE’S EXPERIENCE runs the gamut from leading small groups to large-scale tactical planning. He led seal teams during some of the marquee moments of our nation’s history, such as Desert Storm, Bosnia, Mogadishu, 9-11, and Haiti. He has also commanded several critical hostage rescue operations, one of which became the basis for the movie Captain Phillips.

Since commanding the United States Naval Special Warfare Development Group—known as DEVGRU—Moore served as the director of counterterrorism on the National Security Council and the deputy director for special operations at the Pentagon. Calling Moore “truly

The final event of the ASIS International Seminar and Exhibits was a closing keynote by U.S. Navy SEAL Rear Admiral Scott Moore (ret.). Moore was introduced by ASIS President Richard E. Widup, Jr., CPP. “The former commander of the naval special warfare development group, Moore is one of the nation’s most legendary—and most unknown—heroes. He led the military’s most elite forces during one of the most dangerous times in our history. During his distinguished career, he directed more than 2,000 missions and witnessed frontlines that most commanders only hear about.”

Sam Olens, attorney general, State of Georgia.

THURSDAY
The announcement that Atlanta’s Ralph J. Bunche Middle School had won the ASIS 2014 School Security Funding Competition was made at Thursday’s Closing Luncheon. Principal Mario Watkins competed with other administrators from Atlanta public schools for the grant. To be selected for this award, Watkins and his staff submitted answers to four questions related to security concerns as the school.

“As a staff,” he wrote, “We work extremely hard to ensure that safety issues do not impede our students’ academic achievement.” But when evaluating the current security of the school campus, “We are concerned that the absence of cutting-edge security equipment may increase the security risks for our school.”

Watkins explained that approximately 700 sixth, seventh, and eighth graders enter the school in less than thirty minutes each day of the school year, making the detection of incoming illegal or prohibited items difficult. By adding security devices such as an x-ray scanner, Watkins was confident that the school’s ability to find and confiscate contraband would improve the overall school climate and boost student achievement.

These thoughtful answers impressed the judges from the Greater Atlanta Chapter who reviewed the submissions. Monique Wilkerson, CPP, security program manager, HSS Aviation and Government Service, headed the selection process as a member of the Host Chapter Committee.

The School Security Funding Competition was established eleven years ago by the ASIS Foundation as a way to give back to the communities in which the Annual Seminar and Exhibits is hosted. Bunche will receive a minimum of $20,000, a security-oriented career day, and more.
larger than life,” Widup noted that Moore had “commanded at every level, and from the mountains of Afghanistan to briefings in the Oval Office. He is the man our nation’s leaders trust when failure is not an option.”

Moore took the stage to tell the tale of the rescue of Jessica Buchanan on January 25, 2012. She was an aid worker who had been kidnapped by Somali pirates who held her for ransom. After intelligence was gathered that Buchanan was critically ill, it was decided that two-dozen Navy SEALs would attempt a daring rescue. Because of conditions on the ground, it was decided that the best way to get to where Buchanan was being held was by a high-altitude parachute jump over shark-infested waters to avoid rival pirate clans, weather issues, and other problems.

Moore said that he was monitoring the mission via the use of drone aircraft that were silently flying above the pirate camp. He could see on the screen the captors moving around the camp. “That’s how clearly you can see everything going on with drones,” he said.

Moore explained that in hostage exchanges, “It’s all or nothing and everyone on that mission knew they had to assume whatever risk they had to in order to get the hostage out alive.” He said during his career he’d seen missions fail and that when they did, it sometimes resulted in the death of both hostages and SEALs. One way to prevent this was by maintaining the element of surprise. During this mission, however, that element was lost as the team neared the pirate camp. At that point, Moore said that he heard “troops in contact” on the radio and knew the soldiers were going to have to decide quickly whether to move in or abort the mission.

Moore then explained that on every rescue mission “you have a ‘Number One Man’—the first guy into the room where the hostage is being held. It’s the most dangerous and most important position on the SEAL team…. You never know who it is going to be because a lot of things can happen on the way to the target. Everyone in the team has to have trust in each other’s capability to become the Number One Man, if necessary. SEALs often fight each other to be the Number One Man and will trick each other to try to get the position.”

He discussed the kind of person who wants to be the Number One Man, moreover become a Navy SEAL. “He thinks that if anyone gets to fight for his country, it’s him… [and] he has a healthy dislike for authority,” Moore noted.

Training for the SEALs is about who has will, not necessarily great strength, he said. Training is also about the team. Leaders may have the final say, but must have the trust of their teammates. “It’s not about how good you are, but how bad you’re not. You just have to be good enough” to lead. Token leaders get token followers who “say ‘yes, sir’ and then amongst themselves say ‘Here’s what we’re really doing,’” Moore explained to the audience.

Moore stated that “for product-driven companies, you have to decide whether it is okay to have non-team players. As the leader, you have to watch the team dynamics and make adjustments… then you have to force a culture...
ADDITIONALLY, TO RAISE awareness of the event, ASIS partnered with 14 media outlets that specialize in security-related content. These news organizations helped to disseminate important information about ASIS 2014 to various security communities.

Once again, ASIS wishes to thank our sponsors and partners. The Seminar and Exhibits would not have been the remarkable success it was without your support.

PLATINUM LEVEL SPONSORS
Allegion
Tyco Integrated Security
Tyco Security Products

GOLD LEVEL SPONSORS
AXIS Communications

SILVER LEVEL SPONSORS
Allied Barton

DSX
Pelco by Schneider Electric

BRONZE LEVEL SPONSORS
Altronix
Anixter
DAQ Electronics
Europ Assistance
G4S
Gallagher
Identiv Group
Leidos
NAPCO Security Systems
Samsung Techwin America
Securitas USA
ShotSpotter
University of Phoenix

ASIS FOUNDATION SPONSORS
3xLogic
Arata Expositions
AXIS Communications
EPIC Registration
Salient Systems
DURING THE SESSION, Belfor and Lander commented on some underlying trends in security technology reflected in the products that were shown on the exhibit floor. For example, technologies that incorporate analytical tools, which allow rapid processing of information, are on the rise. “You’re going to see the word ‘analytics’ all across the board,” Lander said.

And to enhance user friendliness, more devices are employing touch-screen technologies, whenever possible. “Touch screen is everywhere,” Belfor noted.

However, some programs and applications still require passwords for use—and passwords continue to be a security vulnerability, as they can be hacked. With mobile applications, for example, “security is only as good as the security on your device,” Lander said. Belfor predicted that advances in password technology, and new discov-
**Giles Realized** the complexity of the job, but accepted the position—because “it’s important for Atlanta.”

Understanding that many young security professionals have never been to an ASIS Annual Seminar and Exhibits, Giles and his team wanted to expose them to all that the event had to offer. “We see what we have gotten out of the peer-to-peer interaction, the sharing, the talking,” he says. “We want that for these young professionals.”

What advice would Giles offer to future Host Chapter Committee chairs? “Start early, build a strong team, take lots of notes, and enjoy the experience!” he says.

The following individuals, with their responsibilities, comprised the committee:

- **Timothy Giles, CPP, PSP**, president, Risk/Security Management and Consulting, managed volunteers, set up media and professional tours, acquired favors for the spouses tour, and evaluated session abstracts.
- **Danny Youngerman**, vice president, security technology solutions, Weiser Security Services, Inc., solicited sponsors for the ASIS Foundation Golf Tournament and Foundation Night.
- **Monique Wilkerson, CPP**, security program manager, HSS Aviation and Government Service, promoted the School Funding Competition.
- **Randy Ryan, CPP**, district manager, Allied Barton Security Services, solicited local sponsors for the Law Enforcement and Military Appreciation Luncheon and Foundation Night, bag stuffing, and the prize booth.

The members of this year’s Host Chapter Committee have all previously been chairs of the Atlanta Chapter, and three were on the same committee in 2008, the last time the Seminar and Exhibits was held in the city. In fact, Timothy Giles, CPP, PSP, who chaired the committee in 2008, volunteered to do the same in 2014.
Countless malicious schemes and predators continue to threaten the cybersecurity of websites and computer systems. Attendees of the “Banking and Financial Services—Security Tools and Emerging Trends” Sunday preseminar program were briefed on some of the more widespread scams that are currently circulating.

Denise Anderson, vice president, government and cross-sector programs, Financial Services Information Sharing and Analysis Center (FS-ISAC), highlighted a number of cyberthreats during a presentation on information security and the threat landscape. FS-ISAC is a nonprofit group that facilitates cooperation and information-sharing by those trying to fight hackers.

One example of current threats is ransomware, used by hackers intent on extorting money by disabling computer systems. “They’re basically holding your system hostage, then asking you to pay a ransom, or a fee, to get your system back,” Anderson said. Phishing schemes continue to proliferate; many target systems by sending fake documents, such as bogus court motions, shipping notices, or invoices, which can infect systems. Attackers also continue to improve their methods, and are able to affect more bandwidth in a shorter amount of time. Using a method called drive-by downloads, an unsuspecting user’s system can be infected simply by landing on a site.

In addition to cyberthreats, the program included discussions of other security challenges that the financial industry now faces. Speakers included James S. Cawood, CPP, PCI, PSP, president of Factor One, and James Huskey, CPP, senior vice president and director of corporate security for Wells Fargo & Company.

For security consultants, gaining clients and winning new contracts for services can be a painstaking process. At the “Successful Security Consulting” preseminar program, attendees received a wide range of practical guidance, advice, and tips for building a consultancy.

John White, CPP, the president and CEO of Protection Management
LLC, offered guidance for developing and submitting proposals for jobs and contracts.

Consultants should always remember that bidding is a competitive process, White said. A consultant may be responding to an open Request for Proposals (RFP), or may be personally invited to submit a proposal, if the client is familiar with his or her work. Either way, it’s a good idea to assume that there will be competing proposals submitted.

A significant amount of time and resources should go into a proposal, he said. It should clearly indicate that the consultant’s skills and expertise make him or her the best person for the job. A detailed timeline, and a clear outline of what services will be offered, should also be included.

Perhaps the most crucial advice for consultants, White said, is to avoid mission creep. Both the consultant and the potential client should have a clear mutual understanding about what the scope of the job is, the expected timeframe, and other parameters.


INSIDER THREAT
Leading the discussion for “Developing and Implementing an Insider Threat Program” were instructors Daniel A. McGarvey, director of security programs for Global Skills X-change (GSX), and Christian Conroy, research assistant at GSX. Topics included maintaining an insider threat program, insider threat incident response, and analytics and monitoring.

The instructors led participants through several case studies, such as one where Employee A notices that Employee B is taking a keen interest in some of the company’s classified material. Attendees discussed possible behaviors that could make Employee B an insider threat, and what Employee A should do to report the potential threat.

Overall, both instructors emphasized that a company’s culture is crucial to maintaining an effective insider threat program, and a failing culture will hurt such a program.

HEALTHCARE SECURITY
Attendees learned the importance of conducting security assessments at healthcare facilities on Sunday during the day-long preseminar program “Securing Healthcare Facilities with Future Expectations, New Programs, and Security Officer Implementation.” The program educated attendees on the latest trends, challenges, new and proven security practices, and security officer effectiveness in the healthcare environment. The program was cosponsored by the ASIS Healthcare Security and Security Services councils.

One speaker was Thomas A. Smith, CPP, president of Healthcare Security Consultants, Inc., of Chapel Hill, North Carolina, who discussed the typical elements of a security program assessment and the standards and guidelines that should be considered during the process. Changes in security are often incidental driven and healthcare security professionals should be more proactive in assessing risks before they happen, Smith said. Risk assessments are used to suggest changes in a security plan, especially after a major incident where there is a tendency to overreact.

“It really does take thoughtful analysis of the risks and benefits before implementing long-term change,” Smith said. He outlined a typical healthcare security assessment, emphasizing the importance of making sure the assessment meets regulatory requirements, listing the most common vulnerabilities in the facility, addressing what preventive steps should be taken, and making appropriate recommendations.

It’s also important to understand why the assessment is being conducted and how it compares with previous assessments. Smith acknowledged that it can be difficult to convince senior officials to make the changes recommended in the assessment, so creating an executive summary and conducting a cost analysis of the suggestions may help facilitate change. “You have to find a way to sell [the assessment] to your organization,” Smith said.

SCHOOL SAFETY AND SECURITY

Schools all over the United States and other nations are asking whether they have enough of what it takes to keep their charges, staff, and teachers safe. This program methodically looked at what it takes to assess a school’s security plan effectiveness, as well as how the plan fuses policies and procedures with effective use of technology, pointing out the vulnerabilities and the simple,
but extremely important aspects of the plan that may be otherwise overlooked.

As part of the program on Sunday, attendees participated in a roundtable-style discussion with Donald R. Zoufal, CPP, a safety and security executive with System Development Integration of Chicago. Zoufal spoke about innovative technology and its legal implications during the robust two-day session. Zoufal talked about the pros and cons of emerging security technology in schools, including digitization, bringing-your-own-device policies, video analytics, license plate recognition software, and more.

Such technology has powerful implications for how school security officers can keep students, faculty, and their facilities safe, but also raises privacy and legal concerns, Zoufal said. Technology, such as wearable cameras for officers, can reduce litigation and protect both parties in a confrontation, and video analytics and license plate recognition software can look out for registered sex offenders or others who shouldn’t be on campus.

These sensor systems and digitizing are “two phenomena that are colliding here that the courts are very ill-equipped to deal with, and it causes problems for administrators who are putting together security programs utilizing technology,” Zoufal said. The increased digitalization and centralization of this type of information provides more situational awareness but also requires more access control due to privacy concerns.

Zoufal also led an in-depth discussion of the Fourth Amendment of the United States Constitution and how it applies to issues U.S. school security officials might run into on the job, such as accessing students’ phones or keeping records confidential. He cited a U.S. Supreme Court case that ruled the warrantless search and seizure of cell phones is unconstitutional, but also pointed out that there is no legislation in place to address this issue.

PHYSICAL SECURITY

The preseminar program “Successful Physical Security Projects—Integrating People, Process, and Technology” was held on Sunday. The program, sponsored by the ASIS Physical Security Council, answered questions about available technology, the training needed to operate it, how to measure the selected technology’s performance, and how to manage its operational life cycle. It also discussed the components of a physical security project, available technologies, and their successful integration with people and processes to maximize the project’s success and its longer-term return-on-investment.

Physical security professionals learned how to present a sound business case for their security plans during the presentation “Physical Security Project Planning: Issues, Opportunities, and Return on Investment,” by Jeff Slotnick, CPP, PSP, president and founder of Setracon Inc./OR3M, of Tacoma, Washington, who stressed the importance of presenting a strategic physical security plan from a business perspective in terms that the rest of the enterprise can understand. “One of the challenges we have as security practitioners is how to get senior managers to look at our projects and fund them,” he noted.

Slotnick said one common mistake of security professionals when identifying potential threats is focusing too much on the nature of the risk itself, rather than the consequences of that threat. “It doesn’t make a difference how the chemical spilled...at the end of the day we have a chemical spill, and its impact on people doesn’t change.” He added that being on the same page with the organization’s goals is a key to getting C-suite buy-in. “When you can align your security plan with your business plan, then you have a common outcome, and a reason for management to look at what you’re doing,” he said.

Additionally, Phillip Banks, CPP, director of The Banks Group Inc., talked about enterprise risk management modeling. Any project a physical security practitioner puts into place will have some level of vulnerability to it, and the perception of that risk has an impact on the outcome. Banks noted that risk severity can shift throughout the various stages of a security project. “As we move through any project the risks to the project are not static, the risks go up and down,” he said. “They increase, they decrease—the risks in phase one might not be close to what the risks are in phase two.”

CRITICAL THINKING

The ASIS certificate course “Critical Thinking Skills for Security Solutions” took place Saturday and Sunday. This course provided practical guidance in applying key critical thinking techniques to security problems ranging from sensitive facilities to insider threats, as well as analytic strategies that improve
rigor, defeat mental traps, and increase the clarity of communication. Hands-on exercises and case studies versed students in the use of logic, analysis, synthesis, creativity, judgment, and systematic approaches to gather, evaluate, and challenge information to effectively form decisions and outcomes.

Course leader Kathy Pherson, chief executive officer of Pherson Associates, LLC, told attendees that there are five key critical thinking skills that security practitioners should possess: challenging your key assumptions; examining multiple hypotheses; looking for disconfirming, as opposed to confirming, data; focusing on key drivers that explain what has occurred or is about to happen; and looking for context. She also highlighted the attributes of an effective analyst, which include stopping to reflect, focusing on the message, developing the storyline, preparing the draft, and finally, perfecting the presentation.

Pherson emphasized the analytic traps and mindsets that should be avoided when thinking critically through a problem. The role of memory is important, but should not be overly relied upon. Perception is also influenced by the individual’s background and prior experience. These factors can create cognitive biases that influence the way a problem or situation is interpreted. Pherson also discussed the criticality of collaboration with other professionals, stating that this teamwork is most effective in small groups of eight or less.

**FACILITY SECURITY DESIGN**

What do you do to figure out what you have? That was one of the main questions presented by ASIS Security Architecture and Engineering Council Chair J. Kelly Stewart, managing principal and CSO of Newcastle Consulting, LLC, in “Risk Assessment Approach to Facility Security Design.” Stewart helmed the inclusive presentation by his fellow council members as part of the preseminar program on Sunday morning. During the program, the council explained how understanding the facility security design process is critical for every stakeholder involved in a project to attendees from the United States, Canada, Nigeria, and Trinidad.

The program was originally designed as a three-day course, but the council packed it into a one-day event to give attendees a chance to learn about the design process from inception to implementation and hear best practices before the seminar officially began on Monday. Attendees were also invited to discuss their questions and opinions in an open format, which walked them through the process of conducting asset and risk assessments targeting facility design.

This part of the security design process is crucial as it forces companies and business to identify the risks in the design of their facility and security program. Once these risks have been identified, they can ask the equally important question, “do we need to reduce those risks?” And if not, Stewart says, “Can we accept them?”

If those risks are unacceptable, then companies need to work to redesign their security program to reduce them. This could include making changes through environmental design, adding additional staff, or making changes to the facility itself.

Also crucial to the security design process is an awareness of the design aspects of a facility and an understanding of its footprint. To illustrate this point, Stewart showed attendees a clip of Ocean’s 11 where Danny Ocean, played by George Clooney, walks his coconspirators through the blueprint of the Las Vegas casino they intend to rob to show them what they are up against.

While the scenario is fictional, it shows how important it is for security professionals to have documentation, such as blueprints, to show the specific design aspects of their facility and how those can be infiltrated from the outside, or attacked from the inside. This can help security plan for possible scenarios and develop a protocol to respond to incidents by determining where security personnel should be placed throughout the facility and what they should do in given scenarios. These should also be documented.

Once this protocol is in place, if an incident occurs, security can assess if the actions that were taken followed the given protocol, or if mishaps occurred.

**CRITICAL INFRASTRUCTURE**

The ASIS Utilities Security Council presented the preseminar program “Protecting Critical Infrastructure—from Concept to Implementation.” One of the major changes coming to utilities security is the need for physical security professionals to understand the role cybersecurity plays in the industry, said Council Chair Darren Nielsen, CPP, PSP, PCI, senior auditor of physical and cybersecurity for WECC.

The technology that utility companies use relies on networks, computers, and an infrastructure
that can be hacked. In some cases, hackers will even use physical means to infiltrate computers by coming to the facility and gaining access to technology. In scenarios such as this, it’s crucial that the individual responsible for the physical security of the utility and the individual responsible for its cybersecurity work together to create a response plan that addresses the threat.

Nielsen also discussed the need for utilities to reevaluate their physical security by assessing whether barriers are effective. For instance, many utilities have fences around their perimeter, but these may not protect the facility as individuals can still drive or shoot through them or jump over them, Nielsen explained. Instead, utilities should evaluate whether their perimeter security is really acting as a barrier to keep unauthorized individuals out, or simply as a deterrent.

Council Vice Chair Anthony Hurley, vice president of an investor-owned utility in the New York City area, pointed to another important aspect of utilities security: continually reassessing and improving security plans. Hurley discussed the famous Kaizen method, which was made popular by Imai Masaaki’s book *Kaizen: The Key to Japan’s Competitive Success*, as an example of continuous feedback on how to improve processes and make them more efficient.

This method was developed as a Japanese management concept for incremental change, assuming that every aspect of life deserves to be constantly improved. By adopting a similar policy for security in the workplace, security professionals can routinely make changes to improve processes based on the input of other individuals affected by those changes.

In turn, including others—even those outside of the security department—makes everyone in the workplace feel more involved and allows them to see the value in the current security solution that the business or company is using.◆

Educational Sessions for Every Area of Security

During the educational sessions at the ASIS International 60th Annual Seminar and Exhibits, security concerns on the top of every attendee’s list were discussed by both ASIS and (ISC)², which collocated its Annual Security Conference with the Seminar and Exhibits. All registered attendees could attend both ASIS and (ISC)² sessions with no additional fee.

ALL SESSIONS WERE grouped into tracks and given an experience level that best matched the session content. The approximately 220 ASIS sessions were organized into fifteen tracks; most aligning with the topics covered by ASIS councils, such as information security, investigations, and physical security. Others addressed topics of interest to security sectors such as homeland security, government/military, and system integrators.

The (ISC)² Security Congress complement of 77 sessions added another nine educational tracks of specific interest to IT security managers. The topics related to specific business sectors such as healthcare security, various business applications such as cloud security and digital forensics, and IT concerns such as malware and governance, compliance, and regulations.
A small drone was part of a session on emerging security threats.

Angela Nino, an investigator at Wicklander-Zulawski & Associates, is an experienced interviewer and often instructs on the topic of preemployment screening. She presented attendees with helpful tools and techniques that can aid employers in getting the truth about a candidate’s history—even information that is not on their application. “Applicants will disclose information if they believe that you’re going to find out anyway,” she noted. “If they don’t tell me now what I might find later, they’re not going to have the opportunity to explain that.” Looking for behavioral cues, such as nervous tics when an uncomfortable question is raised, is a good indicator further questioning on a topic is needed, she said. For example, when asking a candidate about recreational drug use, if the person fidgets or gives a verbal response before it is their turn to speak, that could be a sign they have more to reveal about their behavior.

Rationalizing the behavior in question also helps a job applicant to open up, such as using the phrase “no one is perfect” before asking about their criminal history. “If we rationalize as we go into a question, it helps them feel better when they answer that question,” she said.

Nino also suggested asking open-ended questions that start with words like when, where, why, and how, which will evoke a more lengthy response from the applicant. “Letting them do most of the talking is key,” Nino noted.

Nino reassured participants that if they use this effective interview process, the best candidates will rise above the others. “If you’re looking for reasons to like them even though these other bad things exist, don’t hire them. Good people will qualify themselves.”

THREAT ASSESSMENTS
In the education session “Conducting Threat, Risk, and CPTED Assessments in the 21st Century,” speakers outlined the key steps in making a threat risk assessment, as well as some of the physical security concepts of Crime Prevention Through Environmental Design. Inge Sebyan Black, CPP, senior national account manager, Stanley Convergent Security Solutions, said that she breaks down a threat risk assessment at its most basic level to three questions: “What can hurt me?”, “How bad can it hurt?”, and “What can I do about it?” “It sounds very simple, but that can also be really involved,” she said.

Then, when conducting an actual assessment, five steps should be followed: identify all assets, locate weaknesses, identify vulnerabilities, gauge the likelihood or probability of the threats, and sketch out the potential impact of the threat. Different potential threats can also be classified as minor, moderate, or severe.

Other speakers included Lawrence Fennelly, president of Litigation Consultants, Inc; and Marianna Perry, CPP, training and development manager, Securitas Security Services USA, Inc. The session was sponsored by the ASIS Crime and Loss Prevention Council.

INVESTIGATIONS
Corporate investigations can be a daunting task in today’s global society, but developing valuable resources and contacts can make investigations more manageable, said Siti Subaidah Naidu in a joint presentation Monday afternoon.

Naidu, past president of the World Association of Detectives and a founding member of the ASIS International Malaysia Chapter, presented “International Corporate Investigations: Success Is Easier Than You Think” alongside Eugene Ferraro, CPP, PCI, chief ethics officer of Convergent, Inc.

The two focused their remarks on teaching attendees of the Seminar and Exhibits how to traverse legal minefields and the value of developing trusted resources outside of one’s home country.

Naidu noted that private investigators are still relatively unknown in the corporate world in Asia. Few are employed. “Corporate investigation is still very, very new. It is very much a legal or financial institution kind of work, but the scope is great,” Naidu explained.

Often, the work that corporate private investigators do is undertaken by the finance department, which is responsible for ensuring
that companies are performing due diligence. However, private investigators in the corporate world can “provide backup” for the federal authorities, who are often focused on criminal investigations instead of business ones.

Aiding in this backup role are relationships that private investigators can develop with resources in other countries.

Also, from a commonsense approach, developing contacts in foreign countries that can act for you, especially in Asia, can help with the bottom line as investigators don’t have to pay to send a colleague to the country to do research. “Your extended arm can do a lot for you,” Naidu said, from interacting with clients in person, providing additional contacts within the country, or providing a reference of regulations applicable to that nation that differ from U.S. and European standards.

For instance, data privacy laws vary widely from the United States to Europe to Asia, and some types of information, such as tax refunds and criminal records, may be legal to obtain in some places but illegal in others. Having a resource that understands this, and can help investigators move through the red tape, can quickly become an invaluable tool during a high-stakes investigation.

Additionally, understanding what types of information are legally and ethically obtainable can help investigators tailor their “shopping lists” of information they’re looking for in various parts of the globe. This can also prevent corruption in the future if investigators are aware that information they acquired was obtained illegally by a resource.

HEALTHCARE SECURITY

The Affordable Care Act (ACA) does not target the security industry, but it will impact companies when they implement a cost-effective solution to the Employer Mandate on January 1. To illustrate how companies can maintain or achieve compliance with the ACA, Eddie Sorrells, CPP, PSP, presented “How the Patient Protection and Affordable Care Act Affects the Security Industry,” on Monday morning.

Sorrells, COO and general counsel for DSI Security Services, is the author of the ASIS white paper on the Affordable Care Act. He brought a unique perspective to ACA compliance as he has a law degree and 24 years of experience in security. In his presentation, Sorrells addressed the most important challenges facing contract security companies as they work to maintain compliance with the ACA.

The ACA was signed into law in 2010 and many of its major reforms have already taken place, such as the Individual Mandate, or will take place in 2015. Sorrells highlighted some exemptions in his presentation, explaining that the Employer Mandate will not apply until 2016 to employers with at least 50 but fewer than 100 full-time employees if the employer provides an appropriate certification that is described in the ACA rules. These employers must also offer coverage to at least 70 percent of their employees in 2015 as one of the conditions for avoiding an assessable payment. This will then be upped to 95 percent in 2016, or employers will be subjected to fines.

One difficult aspect of becoming compliant with the law for contract security providers is that there can often be confusion about whether security officers are full-time employees under the ACA.

Under the ACA, full-time employees are classified as employees who are reasonably expected to work 30 hours or more each week. Security officers, however, often have variable work schedules and can sometimes be regularly under or over that 30-hour mark.

In some instances, to avoid providing health insurance for security guards, companies will attempt to limit all guards to less than 30 hours per week. However, Sorrells said that companies should think carefully before adopting this policy as it could result in higher turnover rates and training costs, and has the potential to impact client relations if guards are limited in their work hours.
Some alternatives to this strategy that Sorrells offered are limiting the number of full-time officers, not offering compliant plans and paying the ACA penalties instead, dropping spousal coverage, offering security officers full-time health coverage regardless of their hours, or a combination of approaches.

Sorrells urged that companies need to work with their legal counsel, insurance providers, and accountants to find a solution that best meets their individual needs.

**Maritime Security**

Attendees heard about recent changes in regulations that dictate maritime security operations during a Monday session with Laura Hains, CPP. About 90 percent of everything bought and consumed in the United States arrives in the country by vessel, so cargo and container security is more important than ever, said Hains, a security consultant and U.S. Customs and Border Patrol veteran.

There are three main standards that dictate security for ships: the Safety of Life at Sea (SOLAS) Code, which was the first set of ship construction guidelines created in 1914; International Maritime Organization (IMO) Code, created by a United Nations special agency; and the International Ship and Port Security (ISPS) Code, which enhances security measures.

Each standard has been updated during the last century because of new threats and issues, Hains explained. SOLAS recently added additional guidelines focused on making vessels more environmentally friendly, and ISPS now requires training and equipment to use when recovering a person from the water—which happens on cruise ships more often than is reported, Hains noted. Regulations for lifeboat release equipment and communication between firefighters on board were also passed recently in response to disasters such as the wreck of the *Costa Concordia*.

The Cruise Vessel Safety and Security Act (CVSSA) established requirements to ensure the safety of passengers and crew, including standards for documenting crimes, resources onboard for sexual assault victims, and railing height requirements. However, Hains said the CVSSA, which was passed in 2010, is not enforced because the training is neither realistic nor useful.

Another security concern is how well containers are screened and scanned. The Security and Accountability for Every Port Act dictates that one hundred percent of cargo containers should be screened or scanned, but this is not effective, Hains said. The scanning process, which often involves tracking cargo on a computer system, was not meant to be a terrorism deterrent, Hains noted.

**Business Strategy**

On Monday afternoon, in the session “Creating a Corporate Security Strategy Aligned with the Business Strategy,” Malcolm Smith, CPP, group head of security and safety services for Nedbank, Ltd., explored the idea that security is both an operational and a strategic activity, and that strategy must be consistent with the business objectives of the organization.

Smith showed how a range of analytical models, including a resource analysis, a value-chain analysis, and an industry analysis, could be mapped out and then fed into an overarching strengths, weaknesses, opportunities, and threats (SWOT) analysis for a company. The findings in the SWOT analysis could help form an alignment model, so that a company’s business strategy, security strategy, and operational plan can all be properly aligned. For example, if one objective of business strategy is to reduce costs and grow revenue, and the security strategy is to maintain security operational excellence, then an operational plan aligned with those objectives may be to use a value-based procurement system that saves money but does not compromise performance.

**Investigations**

Conducting a workplace investigation can start at the human resources department, but it has the potential to end up in a court of law. The ubiquity of mobile devices makes the information subject to litigation seem practically bound-
You’re looking for may not be there,” noted Andriulli. “And it depends on the phone, manufacturer, and model.”

**PRODUCT PIRACY**

Several years ago, Michael Moberly had a conversation with a senior official in agricultural development from a developing country. Their discussion, though brief, has stuck with Moberly ever since as he has researched product piracy and intellectual property theft. “You have something I want and I’m going to get it,” the man said to Moberly, referring to pirating agricultural GMOs. “But when I get it, I can mitigate hunger and starvation in my country and save millions.”

Regardless of the motivations behind the act, the theft of intellectual property and product piracy continues to be a problem for numerous companies. Moberly explained this challenge in his presentation “Product Piracy: A Global Economic Risk” on Monday afternoon, saying corporate espionage is an “extraordinary issue” that’s “not going away any time soon.”

This is partly because the Internet has made it easier to steal tangible and intangible assets from companies than ever before. Also, intangible assets—such as intellectual capital, relationship capital, and structural capital (processes)—are becoming more valuable to companies, estimated to make up at least 80 percent of businesses’ value. These values are not recorded on balance sheets or in financial statements, but if stolen can have a huge impact on the company’s ability to compete in the marketplace.

Further hindering companies’ ability to protect themselves from corporate espionage are the number of policymakers, company C-suites, and management teams who struggle to “get their arms and heads around” precisely why cybersecurity and economic espionage prevention initiatives are essential from the outset of any business initiative, Moberly explained. This, along with the prevalence of cyber-economic espionage, can produce substantial—if not debilitating—effects on a company’s value and its sources of revenue, profitability, competitive advantages, growth potential, and overall economic sustainability.

Despite the prevalence of corporate espionage in society, some reports seem to dramatize the costs and losses attributed to cybercrime and economic espionage. Moberly said that he has read every major study on the topics in the past 25 years and has found that they are “somewhat competitive” in that they appear to broaden the ranges of dollar losses and adverse economic impacts.

One study he mentioned that backed his findings was released by the Center for Strategic and International Studies (CSIS) and McAfee in 2013. After the study was completed, CSIS Director for the Center for Technology and Public Policy Program Dr. James Lewis said he believed that “the upper limit of the costs-losses attributed to cyber-economic espionage might be somewhere under one percent” of the world’s gross domestic product. However, this still could correlate to losses, specifically attributed to China, reaching as much as $140 billion annually or 580,000 jobs.

**TERRORISM**

There is a lot of fiction that needs to be separated from fact when it
comes to terrorists crossing into the United States from Mexico, said border security analyst Sylvia Longmire during a Monday afternoon session. Understanding what threats are real is important to keeping the country safe and using resources wisely. And although tales of extremist Muslims crossing the border from Mexico to the United States make good television, Longmire stressed that analyzing both sides of the story is crucial.

There are between 20,000 and 40,000 Muslims living in Mexico, but the presence of Hezbollah members in the region is unknown. However, thousands of Hezbollah sympathizers have been entering the United States for years, Longmire said, but typically just to raise money for the cause by selling knockoff goods.

“People don’t know about them because they’re not blowing stuff up, they’re just making a lot of money,” Longmire explained. “No operational members of Hezbollah have ever been arrested, just folks who have been coming here to raise money. If you’ve ever been to any major city and bought a fake purse or shoes or anything, there’s a good chance that money is going to a terrorist group.”

Longmire said it’s hard to nail down the number of Muslims entering the United States via Mexico, but looking at Special Interest Alien (SIA) and Other Than Mexican (OTM) numbers—classifications for people caught crossing the border who aren’t Mexican citizens—can show helpful trends. For example, the number of OTMs has been historically low, but last year there were more OTMs than Mexicans caught crossing into the United States.

SIAs are people from specially designated countries—often based in the Middle East—who might pose a security risk to the United States, Longmire explained. The immigration patterns of SIAs can give clues to what’s going on in the region. Over the past two years, Somalis and Iraqis have been seeking asylum from the strife in their countries. This is typically given to them, but Longmire warned that extremists from the two countries may be sneaking into the United States with real refugees.

“Every now and then, you see a news report about a rancher where they find different artifacts along the border and it gets into the news cycle and they’re like, ‘Oh my god, I found this on the border, this is certain evidence that we’ve had terrorists crossing from Mexico into the United States!’” Longmire said.

She gave a number of examples of such “evidence,” including photos of an English-to-Urdu dictionary, a crumpled prayer mat, and extremist military patches, which went viral and fueled speculation of an imminent threat. However, the dictionary was intended for an English speaker to learn Urdu, the prayer mat was actually a soccer jersey, and the patches were from a defunct anti-Islamist air brigade.

Longmire also debunked a story about Iranian extremists working with Los Zetas, a Mexican drug cartel, to assassinate the Saudi Ara-
bian ambassador in Washington, D.C. She said the plot was thought up by two men and was never financed or approved by Iranian officials, and Los Zetas was never involved at all.

HOSPITALITY SECURITY
In the world of hospitality, no two venues are the same. “Every place is as different as a fingerprint,” said Russell Kolins, CEO of Russell Kolins PI PC, and the culture of an establishment, its location, its entertainment, and its owner’s philosophy are integral to understanding the security needs of each individual venue.

Kolins focused on that topic in “Hospitality Security: Mistakes Made, Lessons Learned,” which he copresented with Leslie N. A. Cole, Sr., CPP. In their presentation, Kolins and Cole discussed some of the common missteps that owners make in the hospitality industry and how those can be mended to create a more secure environment for patrons and employees.

Kolins also discussed the need for written documents detailing the proper procedure for evicting a patron from an establishment. If these rules aren’t documented, employees need to know the proper procedure and how to execute it. Writing the policy down may or may not be a good move for a business, depending on advice from its legal counsel, “but knowing the rules and how to enforce them is extremely important,” Kolins explained.

He also said that bouncers in the hospitality industry “don’t need the big biceps.” Bouncers should be professionals with good communication skills that can “get the job done.”

LEGAL ISSUES
Instead of presenting a mock trial as they have done in previous years, Barry A. Bradley and Gary J. Bradley of Bradley & Gmelich spiced things up with a series of mock depositions.

In “Defending Security Policies and Practices at a Deposition,” the Bradley cousins, who specialize in security law, deconstructed security policies and practices during live depositions and video clips of real encounters between a security officer and a grocery store customer.

Assisting in the presentation by acting out the mock depositions were ASIS Board of Directors Chair Geoffrey Craighead, CPP, vice president of Universal Protection Service; Bonnie Michelman, CPP, director of police, security, and outside services for Massachusetts General Hospital; and Roy Rahn, CPP, vice president at Universal Protection Service.

While acting out the depositions, the Bradleys showed the tricks and tactics lawyers use to persuade juries and how security companies can craft their documents and practices to avoid or minimize after-the-fact scrutiny that results from a civil suit.

CYBERSECURITY
Cynthia Hetherington, president of Hetherington Group, told attendees Tuesday why they might want to double-check what they’ve shared publicly on social media. This advice was offered during the session “Resources for Monitoring the Internet for Threats.” As a cyberinvestigator, Hetherington says it’s easy to find a plethora of professional and personal information online, even if someone has privacy settings enabled on their social media accounts.

“Everyone’s all worried about people looking at their Facebook accounts,” Hetherington said. But the easiest way to find information on somebody? “LinkedIn. Now that’s what we’re looking for in this environment. From there, we start getting to the other things that I want to find out about you. These are the leads that I’ll use to track you down.”

Even a mention of a hobby, sport, or supported cause could give people like Hetherington enough information to find other online accounts. “I don’t hit the gate, I look for the open window around the back,” Hetherington noted. “Even if you’re locked down and very secure and don’t talk, your kids do or your spouse does.”

This type of passive monitoring could spell trouble for businesses trying to protect themselves from hackers and competitors looking for intellectual property, as well as loose-lipped executives who post personal or travel updates online.

It can also be used as a tool to monitor employees, Hetherington explained. She showed the audience examples of employee profiles that inadvertently shared insider company information or showed signs of violence, which could be critical in stopping an attack by a disturbed coworker before it happens.

Hetherington said that if companies are planning on screening or monitoring employees using social
media, they should develop a policy to protect themselves. Legally, social media monitoring is ambiguous when it comes to privacy concerns because so many people voluntarily share personal information online.

**VIDEO ANALYTICS**
During the Tuesday educational session “Creating Force Multipliers with Video Analytics and Uniformed Security,” participants learned about utilizing video analytics to decrease costs and increase workforce effectiveness.

Cale Dowell, Thrive Intelligence, discussed using video analytics in a more robust, proactive way that can help eliminate the need for someone to monitor multiple video feeds. “There are a lot of human errors that can be introduced when keeping human eyeballs on a video surveillance feed,” he said, noting a published statistic that said after 22 minutes of continuous video monitoring, an operator will overlook up to 90 percent of onsite activity. With video analytics, video surveillance can be used to work for the end user in a more cost-effective way. “You can get that person back from behind the desk and in the field.”

Dowell pointed out the differences between motion detection, which alerts when there is a pixilation change, and video analytics, which watch for specific, triggering events that alert the security operator. “Analytics only focus on the target,” he said.

The session also highlighted current industry challenges, including increasing security while simultaneously controlling costs, keeping up with the new technologies that are available, and applying them in a way that reduces dependency on labor without reducing security. Dowell pointed out that many organizations are leveraging video analytics for operational security and marketing purposes, as well. “With analytics, you’re getting access to a few more budgets, it’s not just security,” he said.◆

Shostack used George Lucas’s *Star Wars* universe to illustrate his point: that threat modeling is not only extremely important, but also fun.

“Threat modeling is the use of abstraction to get to the essence of the security questions we care about,” he explained. “So how do you threat model? Over the years, there has been a lot of complexity poured onto it. We’ve made it difficult to do; we’ve made it intimidating; we’ve put these complex steps that no one understands at the front of these processes, and as a result, people feel stymied; they feel it is difficult to actually engage in effective threat modeling, and that makes me sad, because threat modeling is fun, easy, and it’s the
best way to be sure that the things that you are designing, building, and deploying are secure from the get-go, rather than trying to bolt security on from the other end of the process.”

Shostack discussed in detail four questions that a systems designer can answer: “What are you building?”, “What can go wrong?”, “What are you going to do about it?”, and “Did you do an acceptable job?”

To help determine the answers to the second question, Shostack presented a mnemonic called STRIDE, which stands for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. He said it is a useful way to think about what can go wrong that doesn’t require a book, checklists, or documentation to guide the way. He then worked through all of the potential threats that make up STRIDE, providing examples out of Star Wars, such as that spoofing could be Luke Skywalker pretending to be an imperial storm trooper or that tampering might be Obi Wan disengaging the power supply to a tractor beam, or that the whole story arc of the movies was about information disclosure and its consequences rather than the coming-of-age story of Luke.

“Each STRIDE threat has an inverse security property that you want your systems to have,” he said. For example, spoofing is the opposite of authentication and tampering is the opposite of integrity. Designers should apply these technologies to the system they are building to defeat the STRIDE threats and thus drive security through the entire development lifecycle.

He also presented the top ten lessons he’s learned helping people do this work. They took the form of traps. Among them were not telling developers to think like attackers because it doesn’t provide people who lack that skill with any clear instructions, or that there is a monolithic method to threat modeling—it is more a case of having small methods that interconnect like the Lego snap-together Star Wars characters and props Shostack used during his presentation.

PETERSPECTIVES ON SECURITY

This year, the Perspectives on Security session looked at “Security Executives and the Fight Against Corruption.” The session was moderated by Frank Ewald, CPP, vice president of corporate security for Deutsche Post DHL, who began by noting that “Corruption is not a problem just for economic growth, but for society in general.” The watchdog group Transparency International has found that there is corruption in every nation of the world. Lawmakers have been challenged to draft legislation that fights it, such as the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act. But private organizations must play a role in defeating corruption, too.

On stage to debate the topic were Michael Bouchard, CPP, chief security officer, Sterling Global Operations; Michael Scher, senior editor, FCPA Blog, and an attorney; Sulasksh Shah, director of forensic services, PricewaterhouseCoopers, LLP; and Christoph Rojahn, director of forensics, Deloitte & Touche.

Bouchard explained that with the U.S. law, there are notable gray areas. Perhaps most troublesome is what does or does not constitute an illegal facilitation payment. “It can be tough to judge,” he told the audience. “It’s ill-defined. If you are going to a country and you need 200 visas and you need them in two weeks, [the foreign nation] may say it’s going to be 30 to 60 days unless you move them to the top of the pile for $25 per visa. If you have your papers in order and you would have gotten those visas anyway, then the expediting fee is okay. In some foreign countries you won’t get a receipt for this, but you should ask for one to prove that it is an acceptable facilitation payment.”

Scher told attendees that when he began his career not so long ago, there were no compliance offices—not even in financial institutions. “We were more concerned with money laundering,” he said. However, that has significantly changed today.

Scher said that he had three takeaways for the session: First, look for problem; second, study it; and third, find allies in the company to support finding someone to fix it. “Don’t let this be the smoke that turns into a fire,” he warned, adding that law
enforcement prosecutions of corruption cases are increasing in the United States. "There have been cases in the newspapers and many more are coming."

Companies frequently get into trouble, he said, not because of their own actions, but because of those of their subsidiaries. For example, this can happen when the sales people of a subsidiary engage in bribery in a foreign country because they are not working under the same controls as company salespersons would. "They say, 'Leave it to us. We know how to do business in this country,'" he told the audience.

Another area that could result in legal troubles for organizations that fail to do due diligence is when they acquire other companies. The buyers should ask "Do we really know this company?" Scher said. "Because their liability becomes your liability."

He also noted that if a company does have to resort to a bribe because of circumstances that may be out of its control, it should be honest about it. He said that one company paid a bribe to get a kidnapped employee released. In that case, the company did the right thing by putting down in the books that the payment was, indeed, a bribe. "And the regulators were fine with that," he noted.

The next speaker, Shah, who has helped companies build anti-corruption programs, discussed what could go wrong with them. One issue is when companies do a corruption risk assessment, but focus only on issues in nations where they have a large business share. For example, if the company only does 10 percent of its business in Africa, it may be easy to forget that this is a problem zone for corruption and that the odds are greater of the company making a misstep there. One way of proving to regulators that a company is actively trying to prevent corruption, even in small markets, is to send a team there regularly to check on compliance.

Shah stressed the importance of documentation. One example he presented was of a pharmaceutical company that gave large discounts in some countries and then increased the discounts even more. In this case, it was a genuine way to increase business in the region, but without research and documentation to prove this, the company could have been in trouble.

Another area where companies can flounder is "willful blindness or conscious disregard," noted Shah. He provided the example of a U.S. fashion icon "who was trying to become a passive investor in an Eastern European consortium." The leader of the consortium was a man who, if the investor had merely Googled his name, would have immediately been identified as having engaged in bribery to win business. His nickname was, in fact, the "Pirate of Prague." This did not sit well with the jury that convicted the investor on corruption charges.

The final speaker, Rojahn, said the eternal question of compliance is how to adhere to relations without hindering business. And this eternal question is being addressed in organizations where the traditional security function is undergoing a transformation and repurposing into a unit that mitigates all risks. He spoke about the evolution of compliance within major companies. Today, "Compliance and security within most organizations are very separate and significant functions," he said, adding "I have clients who have literally built up compliance departments of several hundred people over the last ten years."

A perennial issue that does not seem to change, even in the face of change, is that due diligence investigations are a complicated process encountered where the lines between public and private corruption are more blurred. Even in nations with a strong anticorruption focus, such as Germany, financial institutions that are jointly publicly and privately owned are hard to regulate.

Due diligence also becomes harder and sometimes nearly impossible the further away a company operates from its home nation. Rojahn told the audience that he's heard it argued that there are some nations where a business will never be able to get the information and documentation it needs to
prove it was compliant—and if it does, the information was obtained illegally. If this is the case, companies need to make truly tough decisions about whether to pursue business in these nations.

SECURITY INSIGHTS
The third of the Thursday sessions was the Annual Security Insights Program, this year titled “An Insider’s Look at China.” The guest speaker was Evan Osnos, a correspondent for The New Yorker Magazine. Osnos was based in China from 2005 to 2013 and is a historian of the country’s rise to power and an expert on Chinese culture. With him as an interviewer was ASIS Past President Steve D. Chupa, CPP, director of global security for Johnson & Johnson.

Osnos spoke on China’s rise to economic greatness and its implications for the security community. “This is a moment of complex sentiment about China, because it seems both powerful and, in some ways, vulnerable; it seems to be our opponent but also in a cooperative partnership,” he said.

He noted that the Chinese city-state of Hong Kong was then in a rare moment of political unrest, calling for Beijing to give it greater control over the election of its officials. “How did China get here and what does it say about China going forward? After all, Beijing puts more emphasis on economic development and modulating political stability than any city in Asia,” he noted. “Hong Kong has always provided a window into China…. It can also provide a framework for understanding where China is going.”

He discussed the 1989 democracy demonstrations in Tiananmen Square that ended in bloodshed, but they marked the “dawn of a new period of expectation, and the Chinese people began to talk about what they imagined for themselves. There was moment that always stands out for me when a student in the square said to a reporter ‘I don’t know exactly what we want but we want more of it,’” he recalled.

The economic boom in China has not made all Chinese rich, but it has brought many of them out of poverty. In the past, there was always pressure to conform and to be “a rustless screw in the revolutionary machine,” Osnos said, but now “the change has been profound on people and their sense of self.” In China, there is the onset of economic opportunity, the belief among themselves that that the Chinese are entitled to something better, and that they have individual choice. “This time, people are beginning to say ‘We know what we want and we want more of it.’”

As the Chinese acquire more property, the more they need to protect it. To achieve this, “They need to know who is setting the rules and who is breaking them,” he told the audience. Recognizing this need, the central government has let there be some journalistic investigation and reporting in all forms of media. There is also increasing concern about inflation, about unemployment, and about protecting the environment from the ravages of industry.

In response to a question from Chupa about whether China was headed for another Tiananmen Square, Osnos answered that it is not likely. China in 1989 had smaller economy than Italy. Today, its economy is behemoth and “it cannot afford to have sanctions that lead to a three-year recession, as happened after Tiananmen Square, and it cannot afford to alienate a generation of young people,” he stated.

While the ASIS Annual Seminar and Exhibits is celebrating its 60th Anniversary, one key partner is marking his 30th year working behind the scenes. Charles Ticho, president and executive producer at Performance Designs, Inc., has been providing the direction, scripts, videos, and coaching that result in apparently seamless productions of the week’s opening ceremonies, general sessions, and networking luncheons.

From his podium in the ballroom, Ticho has watched the ASIS Annual Seminar and Exhibits grow to become number 94 on the list of the top 250 U.S. conventions, according to Trade Show News Network. Over the years, Ticho has been ably assisted by his wife, Jean, his children, Robin and Richard, and now his grandson, Michael. Adapting his cameras, sound systems, lighting, and logistics to convention centers in at least 15 cities throughout the United States, Ticho has helped ASIS executive leaders transition from podiums and fixed microphones to teleprompters and lavaliere mikes. He ensures that prominent speakers and performers are well taken care of, meeting any special requirements in their contracts.

More importantly, “his creativity and imagination have introduced new meeting formats that are now mainstays in the overall program,” says Susan Melnicove, ASIS vice president of education. Interactive panels, Socratic dialogue, audience participation, and a focus on current issues during the Security Insights programs have kept the programs fresh year to year.

While looking for new ways to maintain the high quality that ASIS Seminar and Exhibits attendees expect, “Ticho and his professional crew are conscious of providing the best in the most cost-effective manner possible,” adds Melnicove.

During three decades as the man behind the curtain, Charles Ticho has consistently touched all phases of the ASIS Seminar and Exhibits with his special wizardry.