SECURITY LETTER™

A private monthly Letter – plus supplements and data services – on issues of corporate planning and protection

166 East 96th Street, New York, NY 10128 – 212-348-1553 –

October, 2016
New York, NY, Vol. XLVI, No. 10
Part I

CSO'S NEED ANNUAL BOARD PRESENTATIONS TO INFLUENCE POLICY, SUPPORT.

Normally chief security officers (CSO's) have a senior reporting level to HR, the chief internal counsel, COO, or other administrative position depending on the nature of the organization. Relationships with all of these positions tends to be fluid and frequent. That's the way progressive organizations get the work done.

But whether the organization is a private for-profit entity, an NFP or NGO, or the govt., something else is vital. The CSO needs to have facetime scheduled annually with the board of directors, trustees, administrators, or whoever ultimately leads.

This annual report should summarize weaknesses and threats the workplace faces and what measures are being taken to minimize risk. The oral and written presentation focuses on what's on the CSO's mind. An oral report to the board is important so that questions may be raised that reflect concerns of the board.

An expectation for the job. It's not enough for the CSO to be able to meet privately with the CEO, COO, or CoB on reasonably short notice. Annual presentation to the entire sitting board should be part of the job description. It may be in the boardroom or via full-board links. Naturally, if a significant emergency occurs, the board will want to hear from the CSO immediately.

Some boards have heard from CEO's for ages. The reason why *all* board need to provide such access is to receive the latest thinking on cybercrime, security program implementation, changes in training due to evolving circumstances, exec. and board protection, liability, and other issues.

When top security practitioners search for position as CSO's, the opportunity/necessity of a formal, annual board report on security should be raised. If the answer is not positive for such vital communication, the message may be that the CSO is not so important or needs to be controlled.

Y2Q--YRS TO QUANTUM--TO IMPACT GLOBAL INFO SECURITY. PREDICTED: 2026.

Today's encryption likely will be obsolete in a decade, or less. We first mentioned the risks of quantum computing attacks last year. (SL 11/15) We stated: "Quantum computing can process multiple activities simultaneously and will make all current forms of encryption obsolete."

Every credit card, debit card, encrypted ID, and email message will be vulnerable to intel agencies. Soon untold hackers, hactivists, foreign state spies, and routine bad actors will take up the power of quantum attacks. For now, 128-bit or more encryption is desirable. But a decade from now, it is estimated, an entirely new form of encryption must emerge.

Cuing up on qubits. Quantum computing uses principles of quantum mechanics. This is the branch of physics that explains the set of laws governing the atomic and subatomic sphere of atoms, electrons, photons, and other particles. Traditional computers use long strings of bits to encode either a zero or a one. Quantum computing uses quantum bits, or qubits.

Qubits can be in multiple states at the same time (superposition). This is the phenomenon in which

Editorial staff: Robert D. McCrie, PhD, CPP. Contact: rmccrie@verizon.net Luis A. Javier. Circulation manager: Fulvia Madia

pairs or groups of qubits can only be described in relationship to one another even if they are on opposite sides of the universe (entanglement). So quantum computing can be exponentially faster and more capable at factoring large numbers--the basis of current cryptology--thus attacking previous codes.

Coincidentally, quantum computing can result in important advances in science, technology, and engineering just as it's weakening security. Greta Bossenmaier, chief of Canada's Communications Security Establishment (similar to the CIA) told a conference last month: "Nearly every company, nearly every organization, nearly every government currently employs some form of encryption." The conclusion is that all of these organizations "could be vulnerable" if quantum-safe computing is not developed.

CRIME IN THE U.S.: VIOLENT RATE UP 3.1%; PROPERTY RATE DOWN 3.4%. The FBI's annual crime report identified an increase in violent incidents. However, the more numerous property crimes declined in aggregate producing the 13th straight year of collective serious crime declines.

It is often remarked that the US does not have a natl. police force. What it does have is 18,439 city, county, university and college, state, tribal, and federal agencies that participate in the FBI's Uniform Crime Reporting (UCR) Program. The arrest (not clearance) rate for murder and non-negligent manslaughter was 3.5; rape (aggregate total of revised and legacy) 7.1; robbery 29.7; and aggravated assault 117.0 per 100K inhabitants.

The rise of homicide data--10.8%--is clearly disturbing. Over 20 US cities have a murder rate greater than 11 per 100K pop. These incidents are tightly concentrated in distinct areas. Researchers call it, "crime of place." Deaths are race-related: 7,039 African-Americans were killed last year compared with 5,854 whites. Gun violence resulting in death grew from 67.9% in 2014 to 71.5% last year.

EXEC. PROTECTION: MOST DANGEROUS CITIES--MEXICO SAFER; VENEZUELA BAD. One of your editor's former students is bright, resolute, and tough. He is researching homicide in San Salvador, one of the most violent cities on the globe. Among the top 10 nations with the leading number of cities with homicides based on population seven of them are to the south. Countries with the most dangerous cities: Brazil, 21; Venezuela, 8; Mexico, 4; Colombia, 3; Honduras, 2; and El Salvador and Guatemala, 1 each. Others: US and South Africa, 4 each; Jamaica, 1.

In the past year, the number of most violent cities has changed with increased violence in Venezuela, Brazil, and South Africa and decreases in Mexico, and Colombia.

Four cities in the US make the top 50. (See Table.) These communities are roughly 10-times the national average for non-negligent homicide.

A safer nation. Even today some citizens fail to perceive that crime is down. A quarter of century ago, the murder and non-negligent manslaughter rate was 9.8 per 100K pop. Two decades ago the homicide rate had slipped to 8.2, and has trended down since then to the current 4.9.

Liability risks have placed the burden on organizations to avoid dangers that can be reasonably anticipated for workers and customers. Research shows that only distinct areas of cities are the intense focuses of non-negligent homicide and other violent crimes. Managers can and should identify such locations, warn execs. and mgrs. to avoid them.

Failure to provide timely warnings could be negligent.

Most Dangerous Cities in the World

Rank	City	Murder Rate
1	Caracas, Venezuela	119.9
2	San Pedro Sula, Honduras	111.0
3	San Salvador, El Salvador	108.5
4	Acapulco, Mexico	104.8
5	Maturan, Venezuela	86.4
6	Distrito Central, Honduras	73.5
7	Valencia, Venezuela	72.3
8	Palmira, Colombia	70.9
9	Cape Town, South Africa	65.5
10	Cali, Colombia	64.3
	In the USA	
15	St. Louis, MO	59.3
19	Baltimore, MD	55.4
28	Detroit, MI	43.8
32	New Orleans, LA	41.7
	Murder rate in US, 2015	4.9

Murder rate per 100K population.

Source: www.worldatlas.com/articles/most-dangerous-cities Modified 9/19/2016

THAT DAILY ATTEMPT...AND ORGANIZATIONAL RISK--EMAIL PHISHING ATTEMPTS. What once was an occasional risk has soared as an omnipresent pitfall. Phishing attempts or scam emails are becoming harder to judge. Not surprisingly, bad actors are copying logos and improving English,

making it more tempting for victims to be trapped. When that happens, it's often the workplace that is an even bigger victim. Counteracting the risk is the fact that workplaces provide frequent reminders of the risks and sometimes re-training for employees who ease the way for hackers.

The workplace should provide Security Advisories, say, on a monthly basis reminding workplaces of risks and the new tricks being foisted to the unwary or careless. Some basic reminders to workers:

- Avoid clicking on any web link from a suspicious email. That's when the damage starts.

- Be aware of threatening language. *Passwords have to be changed. Arrangements have to be confirmed. Services might be stopped within hours.* Messages like these can easily cause an inattentive email recipient to click-on and follow instructions until it's too late.

- Don't be hooked by genuine logos! Banks, financial cards, and govt. offices send legitimate messages routinely. However, they use non-internet means for contacting the public concerning account closures, verifications, or warnings. Official logos in their correct colors do not necessarily mean anymore that the message itself is genuine. The email address usually is the tipoff of fakery.

- Use care with Internet online registration processes. Online banking is here to stay. Accounts may be opened with bona fide organizations, though never from a workplace computer. When in doubt, use verified phone numbers to ascertain the reliability of the site or the email message.

The usual reminders. The workplace needs to maintain anti-virus and malware programs to the current level of protection. A firewall must be enabled. Passwords that are difficult to crack (8 or more characters including letters and a symbol) should be changed every 90 days.

HUMAN RELATIONS: EFFECTIVE SECURITY OFFICERS MASTER SMALL TALK. Security personnel who interact with the public--that's a great majority of them--need people skills. This is the art of speaking with and relating to the public. This point, seemingly so obvious, is being confirmed by research.

Years ago Claire Raines and Laura Ewing wrote *The Art of Connecting*. They argued that, in an increasingly diverse workplace, communicating well is more challenging and important than ever. Spotting and adjusting to different points of view can make the motivated person a better communicator.

Speaking with strangers can bring positive results. Two psychologists, Gillian M. Sandstrom and Elizabeth W. Dunn, enlisted research participants to talk with fellow train commuters, though they otherwise would not have done so. The result was that they enjoyed the trip more and never were rebuffed. Also, volunteers in London who spoke with gallerygoers at the Tate Modern engendered a happier and more connected experience for visitors. It's the same was with security personnel and their publics.

Small talk is a big thing for security officers. Pleasant greetings, an offer for assistance, and small talk can make the interaction between protection personnel and the public significant on several levels.

The mood of the visitor can be determined. Anxiety can be alleviated. Annoyance for having to wait or other frustrations can vanish. Even an evaluation of a suspicious person can require just a few words. So encourage security personnel to talk with those they encounter.

WARNING ON SAMSUNG'S GALAXY NOTE 7 SMARTPHONES RISKS. As most savvy techies know, Samsung Electronics rushed its intro for its new smartphone in order to beat Apple's new model. Competition is good. But in this case the Galaxy Note 7 had previously undiscovered design issues which could lead to fire from the lithium battery. About 2.5M devices globally need to be recalled.

Samsung Electronics is stepping up to the challenge and replacing them, though supplies will run short for a few weeks. Meanwhile, anyone who owns the model should stop using it until a replacement is available. Danger could occur during and immediately after charging. Employers should instruct workers not to bring the model into the workplace until a replacement is obtained.

TREES SUPPORT SECURITY, AN AUTHOR ARGUES. Joyce Kilmer may never have seen a poem lovely as a tree. But Jill Jonnes states in *Urban Forests* (Penguin Random House) that trees are downright important to a better life in a variety of ways.

During and after storms, trees absorb rainwater, preventing flooding and overwhelming the sewer system. They cool buildings and act as "natural air conditioners." They are beautiful. But the author says that trees also cut crime. How? By making neighborhoods more pleasant, bringing people out into the open, and thus providing more potential persons to deter crime or to serve as witnesses it if it occurs.

BOOK: *THE ETERNAL CRIMINAL RECORD*. American exceptionalism is always a topic to trigger a conversation. A lesser perceived political characteristic is the availability of US court records, particularly related to criminal history. James B. Jacobs, a prof. at NYU's law school, offers the first historical and analytical consideration of the collection and dissemination of such records.

Security and HR mgrs. have a vested interest in this topic. If an applicant has a relevant crim record that is not discovered prior to employment and an incident occurs, the workplace may be held liable for negligent hiring. Indeed, Congress bestowed to the security guard industry a particular law: The Private Security Officer Employment Authorization Act (PAOEAA); Pub L. 108-458 § 6403, codified as 28 U.S.C. § 534. DoJ's implementing regs. are at 28 CFR 6402. This 2004 law permits the FBI to provide criminal history info on prospective employees. (See further mention, Part II.)

Jacobs observes that the collection, storage, and retrieval of crim records is an inexorable feature of US employment and social activity. More information helps decision makers, he commented recently. At the same time access to crim records (which are often erroneous, especially on criminal court dispositions) provides an employment disability to individuals who have committed a crime long ago, but that incident serves to prevent employment. The EEOC's "ban the box" policy allows those with records to move further along in the pre-employment process before a records check may be conducted. What then?

How this all got started. Jacobs says that criminal records became an important issue from two developments: First, the capacity to collect info from hugely disparate sources through computer searches. And the 1993 Brady Handgun Violence Prevention Act, which draws upon the Natl. Instant Criminal Background Check System (NICS), can inform licensed firearms dealers whether the prospective purchaser was disqualified from purchasing a firearm. Response to a query is rapid.

NICS, operational since 1998, draws upon the FBI's Interstate Identification Index, or Triple I. This merges crime records from 18K or so law enforcement agencies. (Triple I has been a factor in more efficient identification of significant records elsewhere in the country when a new arrest occurs.)

Jacobs's tome presents a dilemma. The employer faces pressure to collect crim records for prospective employees. (Jacobs also discusses other records troves used in the retail and real estate markets.) But then, once discovering a past conviction, possibly minor, for a candidate, what to do? Will the employer provide a second chance or play it safe and look for another candidate? Here's a thoughtful book, easy to read, on a major topic. Pub. by: Harvard Univ. Press, www.hup.harvard.edu 396 pp; $39.95.

BRIEFS. End-to-end encryption is more frequently built into messaging apps. But some don't have it and others require an opt-in. End-to-end is provided on Apple's iMessage, Facebook's WhatsApp, and Open Whisper System's Signal app. Opt-in is available from Alphabet's Google Allo and Facebook's Facebook Messenger. Built-in privacy knowledge deserves consideration before messaging apps are selected.

Yahoo is facing mounting criticism that its poor security--in contrast to Google's--led to the loss of more than 500M customer records, possibly from Russian state-sponsored hackers.

Sincerely yours,

Robert McCrie
Editor

SECURITY LETTER
166 East 96th Street, New York, NY 10128

Vol. XLVI, No. 10
Part II

Report on the 62nd Annual ASIS International Seminar and Exhibits

Orlando, FL, the East Coast capital of frivolous entertainment, welcomed (again) a serious crowd for the annual ASIS educational and development event. Perhaps 22K persons were involved in one way or the other at the Orange County Convention Center (OCCC). As usual, the exhibits floor teemed with vendors of products and services and those interested in them. This year a seemingly record number of stress-reducing electronic massage vendors were seeking stressed convention-goers for relaxation therapy .

In 2011, $(ISC)^2$ connected with ASIS. From what we see, the relationship is good, encouraging conventional security practitioners to be more informed about cybersecurity. Conversely, $(ISC)^2$ members learn about physical and electronic extensions into their own fields. ASIS councils do a great job of grabbing people into their booths and interesting them in their specialty security interests. The CSO Roundtable, created for high ranking security practitioners, has been morphed into the CSO Center for Leadership. Some programs are limited to those with elite CSO registration.

Here are some of the highlights from the 270 educational sessions, as well as educational posters and exhibits over the expansive floor of the OCCC:

What Is Expected in an Emergency Response

"First responders" are those individuals who in an early stage of an incident are responsible for the protection and preservation of life, property, evidence, and the environment. Like security personnel. Source: DHS document HSPD-8(2)(d) First responders are expected to arrive at the scene of an emergency within four minutes in 90% of the incidents. Source: NFPA 1710 standard.

To be useful at the time of emergencies, response must be planned, response manuals appropriate and written, drills conducted and reviewed, security involved at all levels. Training of those who could be first responders is critical. Basic needs: First Aid/CPR/AED. For training, see: FEMA/NIMS Series (ICS, IS and G. Also E/L specific position courses) https://training.fema.gov/nims/

Poster Sessions a Plus

Some years ago ASIS began offering poster opportunities. That is, people who had passion, insight, or research on a relevant topic would be able to display their points on a large poster, about 6ft. wide. ASIS's Kay Burgess manages the space. Those invited are also asked to be present for one hr. to answer questions about their work. This year 35 poster presentations were scheduled. It seems to us that interest in these visuals and informal presentations grows every year. Here's a report on four of them:

Preparing transit for threats. Lt. Aston T. Greene, Emergency Preparedness Unit of Atlanta's MARTA, asked "Who Are We Fooling?" Transit systems face security threats. MARTA engaged in a Security Emergency Preparedness Plan (SEPP) to link law enforcement and emergency mgmt. in an effort to achieve enterprise security. A gap analysis determined where SEPP was failing. By then integrating physical, design, electronics, and coordination, MARTA received TSA's "Gold Standard" for its planning, testing, and response.

Waterways for the future. Katherine Harmon, iJET Intl., warned, "Water Security: The Next Global Crisis." Harmon sees water as being a resource likely to be contentious in the years ahead. California is one of seven states dependent upon the Colorado River. Looking to the future, 15 desalinations proposed plants will join three already existing. But these locations are soft targets for terrorists and incidentally costly for the public. She foresees a future water tax when a user exceeds a statistically normal consumption. Harmon has written a white paper on the topic available at www.ijet.com, click under resources.

Typography of workplace violence. Ronald R. Sathre, PB4YGuy, categorize workplace violence into four types: I. Violent acts by those who have no connection with the workplace, that is, external crime. II. The attacker has a legitimate relationship with the organization and becomes violent while being served/serviced by the business. III. Worker-on-worker violence involving present or former employees. IV. Violence committed by someone who doesn't work there but has a relationship with an individual who does, that is, usually domestic violence.

Especially for Type III: The "unlucky 13" early warning signs of potential violence: threats, unreasonable, intimidation and control-oriented, paranoid, irresponsible, angry and confrontational, vindictive, violence fascination, bizarre behavior, desperation, obsessions, substance abuse, and chronic depression. Source: www.workplaceviolence911.com

The "sovereign citizens" movement. David S. Hawtin is a former Tennessee Peace Officer Standards and Training (POST) law enforcement officer, currently with AlliedUniversal. He is concerned about the sovereign citizens movement who are anti-government extremists.

Some are simply time-consuming nuisances. Others are armed and dangerous. An example is in 2013 when two Saint John the Baptist, LA, sheriff's deputies were murdered while investigating an earlier unprovoked drive-by shooting that wounded two of their colleagues. A common feature is their attraction to "debt redemption" seminars. They have convoluted explanations as to why laws of the United States are not valid. Hawtin says that since the 1970's, 78 lives have been taken by sovereigns. Info: dshawtin@united.net

Guarding the Guards

The largest security guard operators convened for the NASCO breakfast which brings together senior officers of the industry. NASCO chm. Jim McNulty reported on the frustration for employers not being able to access criminal records of prospective employees despite passage of PSOEAA. (See book review Part I.) While the federal legislation passed 12 years ago, about 50% of the states have not implemented it. Meanwhile, other private industries like financial and pharmaceutical are able to conduct meaningful searches because legislation has not been enacted. McNulty opines that the solution may be to have a "bundling" service that would facilitate national screening of prospective employees.

Who appears for the NASCO breakfast gives an indication of sorts as to who is making a mark. This year Allied Universal and G4S each reserved eight places, while Securitas had five. (Notwithstanding Securitas has 482 ASIS members, ASIS exec. dir. Peter O'Neil mentioned.) But the biggest reservation came from DHS with 17 places. The breakfast had 111 registrants in total. NASCO has contracted with John Jay College of Criminal Justice to identify, compare, and contrast various state regulations concerning security guards. The database will be completed 12/16.

The Natl. Security Alliance (NSA) convened execs. of 17 member regional guard businesses. Pres. Vic C. Evans observes that the productive relationships among the members offer the potential of providing national resources whenever members encounter need for resources outside of their areas to support clients.

Along the Aisles: Exhibits that Caught Our Attention

Now hear this! While attention to emergencies now involves instant use of social media, audio reports have not lost their place. Talkphone provides a variety of communications devices for security and life safety. This co. has installed educational, mass transit, and life safety communications products across the nation. Towers, wall mounts, surface mounts, and pedestal mounts are available.

A security control center can receive/send messages from these stations. Similarly, messages to an entire area can be broadcast from the control center. Cloud-based web contacts can include text-to-speech and email emergency message transmissions. Remote stand-alone stanchions can be powered by solar system mounts, says David Morefield, sr. sales dir. Info: 773-539-1100. www.talkphone.com

Bringing it all together. Control centers can produce enhanced utility if they are capable of streaming together a variety of data sources. Streaming together is not to be taken for granted. Vidsys Global Security has experience in uniting video, voice, intelligence, traffic, weather, world events, and other data feeds into a coherent whole. Their clients have included: the Republican Natl. Convention, the Boston Marathon, car races in Dubai, and the forthcoming Super Bowl in Houston.

Vidsys CEO and founder James I. Chong explained how the co. works with Hewlett Packard Enterprise, Hikvision, Salient Systems, and Viscount Systems to allow decision-makers control over disparate and fast-moving events. Info: 703-883-3730. www.vidsys.com

Transforming big data. Organizations don't wish even one minute's downtime. Not only are opportunities lost, but also image is crushed as the organization has seemingly dropped the ball.

Qognify (pronounced "cog-ni-fye") provides software to translate big data into situational awareness. Using analytics, the software finds operational intelligence which is then reported to mgmt. Processes can be improved as a result. Trends analyzed. Info: 201-690-5207. www.qognify.com

Track that! Wearable security is a topic of the time. Vismo-alert provides a wearable panic button that connects to a smartphone over Bluetooth. The device does not need to be unlocked for the co. to send an emergency message to all employees. The panic button may be discretely carried.

Users may be tracked via GPS wherever they move. Similarly, adaptation for vehicles can track movements via triangulation. Connection to an Apple Watch is possible. Bluetooth range = 75 ft. indoors; 300 ft. outdoors. Info: 44-(0) 1904-616666. www.vismo.com

Intrusion without excuse. Access control at an increasingly higher level is taken for granted. We noted the 128-bit encryption-protected intrusion detection system (IDS) from CINCH Systems. The UL listed IP-based system encrypts sensors to the control panel via the web. Apart from making IDS's stronger from attack, vehicle barrier control systems have undergone improvement. Info: www.cinchsystems.com

Better barriers. We admired anti-ram vehicle barriers capable of stopping in their tracks a 15K lbs. truck driving 30-50 mph. HySecurity's StrongArmCrash line meets ASTM F2656-07 crash standards, permitting less than 1 meter of penetration. These vehicle barriers may have fewer mechanical problems than wedge control barriers. Opening areas can be configured from 12 to 24 feet in width.

Open/close time is rapid in the 6-8 seconds time. These vehicle barriers come with a variety of accessories such as amber strobe beacons, stops/go lights, vehicle detectors in advance, timers, and photo eye kits to prompt security personnel. HySecurity is now part of TheNiceGroup, Italy. www.hysecurity.com

Advancing classroom intruder protection. The newly opened $50M elementary school in Newtown, CT, has attracted widespread attention. Sandy Hook was the school where a deranged young adult took 26 lives almost four years ago. The old school was razed. A new high-security facility was designed and completed to open last month. Security was a top priority.

"It's essentially a school surrounded by a moat," one recent visitor observed. Inside classrooms and other spaces can be instantaneously locked centrally by deadbolts should an intruder pass the access point. Individual classrooms can lock with a QID (Quick Intruder Deadbolt) by a simple push of a button below the lever, provided by Securitech Group. Mark Berger asked: ”We deadbolt our homes. Why shouldn't we deadbolt our children's classrooms" in the event of an attack? Info: 718-392-9000. www.securitech.com

Virtual reality training. Fuel.Tech demonstrated PerseVR, what they call "the world's first room-scale virtual reality training simulator for real-life emergencies." Volunteers placed a device over their heads and were able to participate, VR-style, in an engrossing active shooter demonstration.

The simulated experience helps participants to confront situations including: workplace violence, industrial emergencies, and natural disasters. Software may be written for specific requirements a client might have. Info: 855-472-7316. www.fuel.tech

Reaction to Terrorism in Orlando: Feeling the Pulse

Among security guard operators, one of the most discussed issues involved G4S, which describes itself as "the world's leading global, integrated security company." The Jupiter, FL-based firm (global hqtrs. is in London) was fined $150K following an investigation by the FL Dept. of Agriculture.

Orlando shooter Omar Mateen killed 49 and injured at least 50 at the Pulse nightclub on June 12. He was employed as an armed security guard for G4S which hired him after a purported psychological screening. The screening was supposedly conducted by Dr. Carol Nudelman, a psychiatrist. But she had sold her practice in Jan., 2006, and Mateen wasn't "evaluated" until Sept. 2007. The investigation claims that Nudelman's name was on 1,500 applications after she had left the state. Mateen worked for the St. Lucie County Courthouse and later as a guard gate at the PGA Village in western Port St. Lucie.

A further complication is that Mateen was on an FBI terrorist list. However, this information never reached G4S. NASCO exec. dir. Steve Amatay asked FBI dir. James Comey a question about sharing relevant records with the industry during an open session. Comey said: "I don't think there's a clean answer. We have to talk to each other about what is possible." Comey said that the Privacy Act prevents the FBI from sharing some info publicly. Separately, Comey stated that Pulse shooter Mateen created terror from his actions but was "not radicalized" in his opinion.

Briefs

AlliedUniversal announced it had supported security officers for the second annual Natl. Security Officer Appreciation Week, Sept. 18-24. AlliedUniversal's Steve Jones noted that one out of every 141 employed Americans was serving as a security officer.

Johnson Controls and Tyco announced the completion of their merger, Sept. 6. The announcement brought out Bill Jackson, pres., Building Efficiency, Johnson Controls, and Joe Oliveri, vp & gm., Tyco Integrated Security. The merger will produce a source for total bldg. management systems, said Jackson. The combination will allow one stop sourcing for: controls, security, HVAC equip., fire & hazard protection systems, lighting controls, operational intelligence, and energy storage.

The unit will also provide bldg. services and parts. The combined entity will produce $30B in revs. and will employ 117K. The integration of the two should result in $1B in merger synergies. As previously announced, Johnson Controls is spinning off its auto business, Adient, on Oct. 31.

One of the biggest crowds on the exhibits floor was attracted by Nightingale Security, which provides aerial robotic security. Their systems use autonomous aerial robots for surveillance cameras and data gathering sensors. The system makes more efficient use of security personnel, noted the sales reps. Info: 415-737-6632. www.nightingalesecurity.com