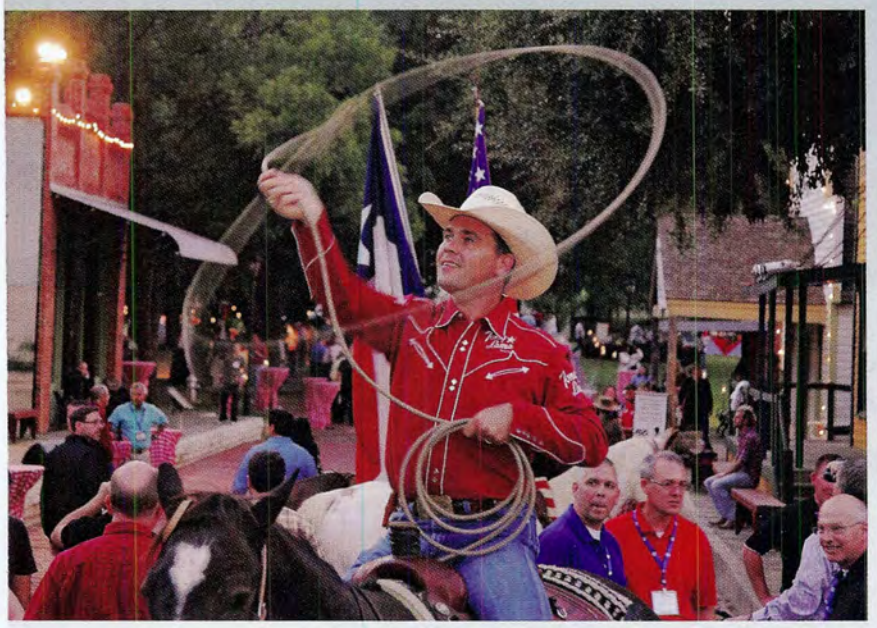
# Courage, Leadership, and Learning



**SECURITY PROFESSIONALS** from around the world gathered in Dallas, Texas, in October to attend the ASIS International 56th Annual Seminar and Exhibits. Keynote speakers offered insights on courage and leadership. More than 170 educational sessions helped to enlighten attendees on topics too numerous to name. Following are some of the highlights. (For in-depth coverage of all seminar events, including products on display in the exhibit hall, see the special seminar section of *ASIS Dynamics* online at www.asisonline.org.)



PHOTOS BY OSCAR EINZIG PHOTOGRAPHY


Assumption #1
Media Will Alter Story to Fit Their Slant
• Decide on Your Message
• Start With Your Message
• Stay With Your Message

KEYNOTE SPEAKERS

# Musharraf Talks Terrorism


FORMER PAKISTANI PRESIDENT Pervez Musharraf during his keynote address

If the United States withdraws abruptly from Afghanistan in the near future, there will be a repeat of the problems that occurred when the U.S. withdrew from Afghanistan in 1989 after a proxy war there with the Soviet Union. The result will be instability with ripples of violent extremism around the globe, former Pakistani President Pervez Musharraf said during his keynote address.

"We are at the threshold of making a decision of whether to quit or not to quit in Afghanistan," Musharraf told a packed hall at the Dallas Convention Center. "I have told you about the blunder of the past. I pray to God that we do not make another blunder."

Musharraf, a former general in the Pakistani army, led his nation from 2001 through 2008, serving as a key ally in the post-9-11 U.S.-led war on terrorism. He currently lives in self-imposed exile in England, but earlier this month, he announced that he had formed a new political party and plans to run again for the presidency in Pakistan.

Despite billions in U.S. humanitarian aid to Pakistan in the wake of the July floods that affected an estimated 21 million, recent polling indicates that 59 percent of Pakistanis view the United States as their enemy. Musharraf traced the sentiment back to the departure at the end of the Soviet-Afghan war, in which Pakistan supported Mujahideen rebels along with the United States.

"People in the streets of Pakistan thought we had been used and betrayed," he said.

While Musharraf said that animosity toward the United States does not imply sympathy for Islamic extremists, the poll, conducted by the Pew Research Center and released in July, found that more than half of Pakistanis have a favorable view of al Qaeda, and 65 percent have a favorable view of the Taliban.

Musharraf traces the persistent political instability and violence in Afghanistan to the coalition's installment in 2001 of Northern Alliance members—tribal Tajiks, Uzbeks, and Hazaras—in government, to the exclusion of Pashtuns, in part because the Taliban consisted exclusively of Pashtuns. Musharraf said he repeats again and again: "All Taliban are Pashtuns. But not all Pashtuns are Taliban."

Key to success in Afghanistan is engagement of Pashtuns and democratic inclusion in government, as a majority. That requires bargaining from a position of strength, which the U.S.-led coalition currently lacks.

After his speech Musharraf told *Security Management* that achieving that position requires direct engagement of Pashtun tribal maliks, or chieftains. With their allegiance, armed Pashtun tribes may be enlisted in the fight.

Addressing counterterrorism, Musharraf—who vehemently opposes the current U.S. military and intelligence operations just inside his country—compared the capture or killing of single terrorists as plucking leaves from a tree, and the elimination of entire terrorist groups to sawing off branches. Elimination of terrorism, he said, requires a holistic approach that incorporates a military element but focuses on three root issues: existing national political grudges, sub-national conflicts, and the persistent lack of education and economic opportunity.

Should Musharraf return to power, he says that his top priorities would be to jump start the Pakistani economy and continue the fight against terrorism, which he says are interrelated, because "The economy means drawing investment from abroad, and investment doesn't come when there's turmoil in the country. We won't be able to succeed in any direction if we don't defeat terrorism and extremism."

In introducing Musharraf, 2010 ASIS President Joseph R. Granger, CPP, who is the security director of the United Space Alliance, noted *Time* magazine's assessment that as president of Pakistan, Musharraf held the most dangerous job in the world. While two attempts on Musharraf's life have been publicly reported, Musharraf told *Security Management* that there have been more. Should he return to Pakistan, he does so a marked man. Rival

PHOTO BY ELIZABETH LANKES

Jamhoori Watan Party (JWP) President Talal Bugti, alleging crimes against humanity, has placed a bounty on Musharraf's head worth $1 billion and 100 acres of farmland.

Asked about the danger, Musharraf remarked lightheartedly that he could use the protection of ASIS's membership. Taking a more serious tone, he told *Security Management* that he has accepted the constant threat of a violent death.

"Maybe I've got thick skin, but I can face dangers. And for the sake of the country we love so much—everyone loves his own country—dangers and risks have to be taken," Musharraf said. "Where there is no risk, there is no gain, as they say. I believe in that."

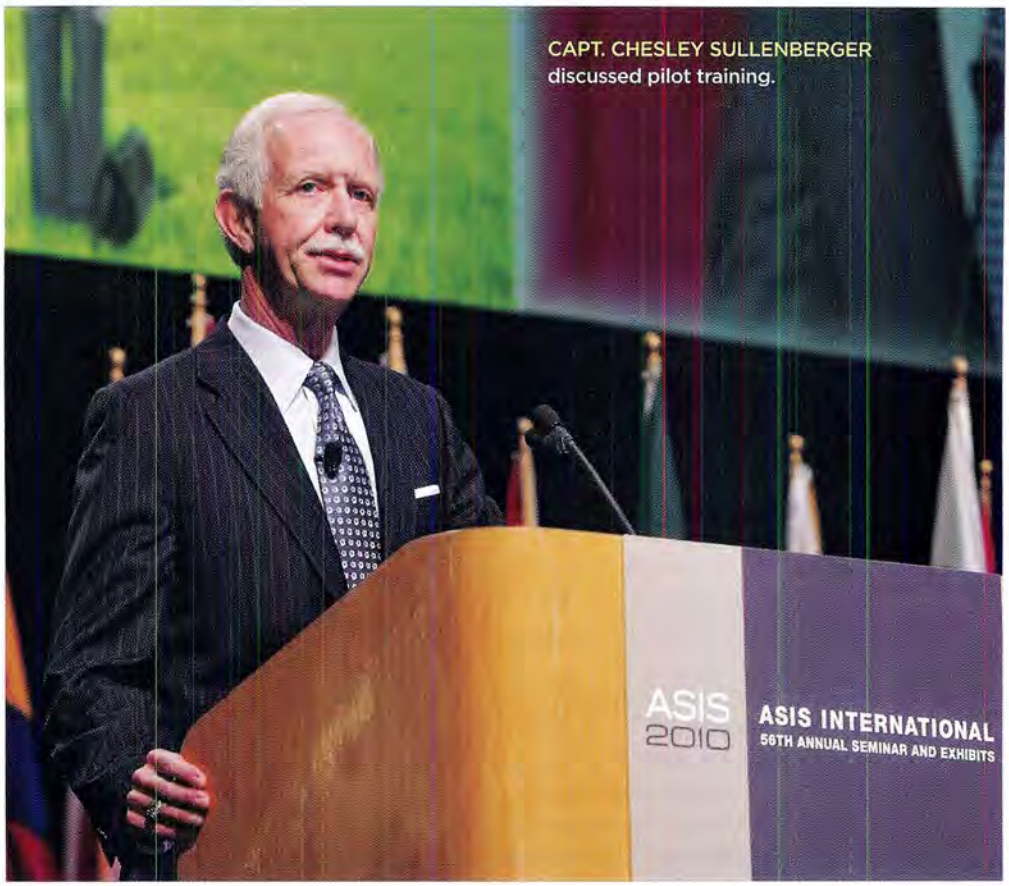
## Sullenberger Stresses Training

The voice over the radio was calm and distinct: "We're gonna be in the Hudson." Moments later, US Airways Flight 1549 landed in the frigid river. Capt. Chesley "Sully" Sullenberger, the man who spoke these words, emerged on stage at the Dallas Convention Center to a standing ovation and launched into a discussion about heroism and why he believed he had the right stuff on that cold January day last year.

Sullenberger told attendees that the two necessary ingredients for his success were education and service. Education has always been important for Sullenberger; the quest for it was instilled in him by his family. He told of how his four grandparents, born at the twilight of the 19th century, accomplished a particularly striking feat: they all graduated from college. He told of how his mother, a first grade teacher, planted a love of reading and learning in him as a boy. He noted how education allows people to learn about the mistakes of others so they don't have to learn the hard way.

"That's particularly true of my profession: we simply can't live long enough to make all the mistakes ourselves," he said. Sullenberger noted that learning isn't just an academic exercise; it's economically vital in today's information-driven world.

Sullenberger next spoke of his parents, both part of "The Greatest Generation," who faced down The Great Depression and World War II, to explain the virtues of discipline, self sacrifice, and service he learned from them, and which he drew on during the Hudson River landing. "They, too, said they were ordinary people who found themselves in extraordinary circumstances," he told the audience. "They also said that they were just doing their jobs. But as we now know through the long lens of history that by just doing their jobs, they saved the world."



CAPT. CHESLEY SULLENBERGER discussed pilot training.

Sullenberger, along with his copilot Jeff Skiles, saved the lives of all 155 people on board the plane that day because of their commitment to their profession and the people placed in their care. "I was a regular guy who had done a pretty good job of preparing himself for whatever might come."

On that day, preparation made all the difference. He and Skiles were able to control the fear rising up in them—the definition of courage, according to Sullenberger. "Fear is normal. Fear is human," he said. "Courage is the discipline and the realistic confidence to do what is required in spite of fear."

What was particularly striking to Sullenberger is how he and his crew's "Miracle on the Hudson" uplifted the nation. In the midst of a deep recession and the nagging fear that American competency was in decline, Sullenberger and his crew's quick thinking and courage gave people faith. "It was seen as life affirming," he said.

Letters flooded his home from every continent, even from a research scientist in Antarctica. "We've achieved Santa Claus status," Sullenberger joked about the burden that his fame placed on his mailman.

Sullenberger is also not one for false modesty. "We did do our jobs exceptionally well," he said. But he expounded the point that doing a good job day in and day out only occurs when the individual feels the necessary drive, discipline, and duty to perform their job to the best of their ability. For Sullenberger, what occurred that day was no miracle, it was the product of a lifetime spent preparing himself for the

PHOTO BY OSCAR EINZIG PHOTOGRAPHY

unexpected. Sullenberger said that the incident was a clear illustration of why professionals' mastery of their craft matters and how it can inspire others.

Since being thrust into the spotlight—although he says "it was lack of thrust" that accomplished that feat—Sullenberger told attendees that he tries to use his newfound influence to better the world. He says past Medal of Honor recipients have set examples he intends to follow. "They will...tell you that in many cases the act that earned them the medal was actually the easier part," he said. "It turns out the more difficult part was living every day in such a way that everyone remembers truly what the medal stands for."

With that in mind, Sullenberger has become an outspoken advocate for aviation safety and his former comrades in the cockpit.

In an interview with *Security Management* after the presentation, Sullenberger expressed his concerns about aviation safety. In the past, he says, the airlines always chose to exceed the necessary regulatory requirements set by the federal government. But in today's economic environment, some airlines have begun to shave down their safety requirements to just above the federal requirements. As a result, he says that the training that helped him land Flight 1549 in the Hudson will become the exception, not the rule.

Already, there are troubling cutbacks. "We're seeing them more closely approach these rock-bottom minimum standards that we never got that close to before, certainly not in my experience," he told *Security Management*. "And so now we have our annual training. We used to do it twice a year, now we do it once a year."

Cost cutting has also migrated to pilot salaries as well. Because of pay cuts and cost cutting, Sullenberger worries commercial aviation won't attract the best and brightest, causing the industry's impeccable safety record to falter.

Before the Hudson splash landing, Sullenberger had to take a 40 percent pay cut, and like many others, he saw his earned pension reduced to pennies on the dollar as the result of bankruptcies in the airline industry. He says entry-level, regional pilots now earn only in the mid-$20,000 range even though they're given incredible responsibility. He is also concerned that pilots are seen as bus drivers because of the outstanding safety record of commercial aviation, although he believes pilots have received much more appreciation since Flight 1549's safe landing.

SESSIONS

## Session Speakers Offer Insight

As security professionals continue to do more with less, best practices are increasingly valuable. Those who attended some of the more than 170 sessions offered at the seminar and exhibits garnered tips and techniques to help meet security challenges. Following are summaries from just a few of the week's presentations.

**Physical security.** Attendees at a session titled "Explosive Threats and Target Hardening: A Study in Explosives Environment Physical Security Response" learned the fundamentals of explosives and how to address the threat from Jeffrey Slotnick, CPP, PSP, president of Setracon Incorporated.

Slotnick discussed risk assessment and planning, including considerations for chain of command, primary and alternative communications, and procedures for locating a suspect or unexploded device.

Attendees also learned about the fundamental science of explosives and how they maim and kill. Primary injuries, Slotnick explained, are caused by the shock wave from an explosion, and primarily affect the ears, lungs, digestive tract, and brain. Secondary effects are caused by debris or collapsed structures. Tertiary injuries, which are no less severe, are caused when victims are thrown by the wind blast from a detonation.

For facility security professionals, mitigating risk means keeping vehicles that might carry larger bombs at an adequate standoff distance from a structure. This can be accomplished with strong fencing, ideally compliant with ASTM Standard F-2656-07, or with bollards, planters, and other measures. Less obtrusive barriers include shrubs and curbs at least 8 inches high. For entranceways, moving barriers—such as retractable bollards and hydraulic wedges—do the trick. Windows should be coated with blast-resistant film.

If a bomb does go off, victims should be repeatedly examined and assessed because of the insidious effects of internal injuries, Slotnick said. While all suspicious explosions bear some threat of biochemical or nuclear dispersal, the risk of traditional injuries far outweighs the likelihood of that or any risk of transmission to caregivers.

JOSEPH L. SMITH, PSP, speaks to attendees about active shooter situations.

PHOTOS BY OSCAR EINZIG PHOTOGRPAHPHY

In addition to tending to victims' needs, officials must ensure that they protect evidence however possible to aid in the investigation and the ultimate prosecution of the guilty party. That means establishing inner and outer perimeters to limit traffic at the scene, and attention to securing "transient" evidence that is either on the victims or subject to quick removal by the elements.

Above all, security staff and first responders should consider the threat of secondary devices placed to strike after the initial blast, Slotnick said.

**Food safety.** Years ago, when U.S. Food and Drug Administration (FDA) employees wanted to start a criminal investigation, they had to follow a long and drawn out process that took "forever," according to George Hughes, senior advisor, counterterrorism and intelligence, in the FDA Office of Criminal Investigations, who led a session on "Food Contamination: A Cross Agency Investigation."

That changed starting in the early 1990s, when the groundwork was laid for the FDA to have its own criminal investigations section, which now includes 29 offices in the United States and about 180 special agents culled from traditional law enforcement agencies. The investigators are responsible for looking into various criminal code violations as well as violations of the Federal Anti-Tampering Act and the Federal Food, Drug, and Cosmetic Act. In recent years, the group's mission has expanded to include terrorism-related investigations.

Hughes said that 85 percent of the department's caseload relates to the manufacture and sale of counterfeit drugs, with China being the country that produces the majority of counterfeit offenders.

Product tampering is another focus of many investigations, although Hughes said that in more than 99 percent of product tampering cases, the perpetrator is attempting to extort money from manufacturers. The cases can originate from a multitude of sources, ranging from the FDA itself to members of the general public calling in tips.

One of the roles of the investigations team is to support the intelligence needs of the various agencies involved in the bioterrorism defense mission. The terrorism aspect of FDA investigations encompasses more than the fear of a terrorist attack or tampering with the nation's food and drug supply. It also involves related issues such as attempts by terrorists to get funds, perhaps via the exploitation of an FDA-regulated product. For example, one well-publicized scheme involved the special supplemental nutrition program for women, infants, and children (WIC); instead of using the infant formula received through the program, recipients sold it to mom and pop grocery stores, with the proceeds on that formula eventually funneled to terrorist organizations like Hamas. Sellers or wholesalers may remove expiration dates or lot numbers from the formula packages or tamper with them in other ways.

**Workplace violence.** When a recession hits and layoffs follow, companies have to prepare themselves for a possible spike in workplace violence. One situation where the threat of violence arises is during an employee's termination meeting.

During one session, Bruce T. Blythe, CEO of Crisis Management International, Inc., walked attendees through how to prepare their managers for terminating potentially violent employees.

One of the first decisions a manager must make is where and when to meet with employees to tell them the bad news. Blythe recommends that termination meetings occur in a conference room, where it's easier for a manager to exit because of the room's size. The ideal situation, however, is to meet outside the company's office so the employee is already off site, like a hotel conference room or an airport lounge. Locations like these reduce the likelihood that the employee will know what's about to occur. It also reduces the chance the fired employee will take out his anger at his former work site, since he's already away from it.

The timing is less significant. If a manager is dealing with a hostile employee, chances are he'll get mad regardless what time of day he is fired. There is one thing to keep in mind, however: Most instances of workplace violence occur on Monday morning, so the conventional wisdom of firing an employee on a Friday afternoon may not have the hoped-for effect of giving employees with violent tendencies time to cool off.

Blythe also recommended that managers set up the meeting room ahead of time. Managers should ensure that a large table separates them from the employee they're about to fire, and they should position themselves closest to the door so that

if things go south fast, they can get out of the room. They should also not put their legs directly underneath the table in case they need to move away quickly. Strong and angry employees could flip the table on a manager, he noted.

Managers should sanitize the room of any potential weapons. Scissors, letter openers, and glass objects should all be removed from the room. Hot coffee is also a bad idea unless a manager wants it in the face. The only refreshment provided should be something that comes in a plastic bottle, because it's unbreakable and tough to weaponize.

**FRANK SCHURGERS** discusses international due diligence.

To keep a termination meeting moving along, managers should prepare a term sheet, which explains when fired employees will receive their last check and any other benefits or severance. By moving quickly down the term sheet, a manager can keep control of the situation. But they should always sit "at the ready," poised to enact their safe escape strategy at a moment's notice.

If a manager has security personnel to rely on, he or she can position them in another room close by in case things get out of hand. Blythe says an easy way to create an emergency communications option is to position a baby monitor or open cell phone somewhere in the room to transmit the conversation. If things get dicey, the manager can call out a code word that brings a security response.

A company should never fire someone over the phone. It's considered provocation, Blythe said.

**Cybersecurity.** Organizations face constantly evolving cybersecurity risks. One of the biggest could include ensuring that remote and third-party workers securely access an organization's network.

That was according to Kevin Goldsmith, IT manager at CA Technologies, and Scott Algeier, executive director of the nonprofit Information Technology—Information and Sharing Center (IT-ISAC), the two speakers at a session on "Managing Remote and Third-party Access to Networks." The pair described access risks and also provided some potential security solutions.

More temporary and telecommuting workers are accessing company networks, said Algeier. He also noted that the Verizon Business' annual *Data Breach Report* found that misused passwords and credentials were the single most common cause of the data breaches studied. Verizon found such misuse in 48 percent of data breach cases.

Algeier suggested some ways that organizations could strengthen their network access management. One way is for organizations to identify their sensitive information, he said. Access to such information should be given only to the employees who need to see it. Any employee leaving a company should immediately have his or her privileges revoked, he said.

Algeier also suggested that more organizations should take advantage of log management solutions. Such solutions can recognize suspicious access activity and many other network-related threats.

Both Algeier and Goldsmith emphasized the importance of training employees in basic IT security practices.

Employees should be trained not to open suspicious e-mail attachments, for example, which can contain malware. They should also learn to be careful about transferring data from one computer to another through devices such as USB sticks, they said, which often infect computers with malware. Some organizations might require that USB sticks be scanned with antimalware software before being inserted into company computers, said Algeier.

**Retail security.** The retail sector offers the kinds of "soft" targets terrorists seek to exploit, but many retailers feel ill-prepared to address the threat. Advice came at a session titled "Behavior Detection and Other Practices for Protecting Retail Facilities from Terrorism," sponsored by the ASIS Retail Loss Prevention Council.

The session featured two officials with the Mall of America in Bloomington, Minnesota, the largest U.S. shopping mall based on retail space. Michael Rozin, the mall security department's special operations captain, presented along with Doug Reynolds, the mall's director of security,



PHOTOS BY OSCAR EINZIG PHOTOGRPAHPHY

and Eric White, director of retail strategy for Wren Solutions.

Reynolds provided an overview of the mall's enormous scale: 4.2 million square feet, 520 tenants, an amusement park, an aquarium, 42 million visitors annually, and $1.8 billion in economic impact. That scope and the symbolic value of the mall's name provide an enticing target, he said.

Rozin discussed the threat of terrorism in the United States, including from homegrown terrorists, such as convicted Times Square plotter Faisal Shahzad and Fort Hood massacre suspect Nidal Malik Hasan.

Amid the threat, the "critical path" for security professionals in the retail sector entails risk analysis, including determination of acceptable risk, influencing critical risks, and preventing catastrophic risks. Practitioners must advocate for risk management internally—without overreacting to the threat. To be effective internally and externally, they must fashion themselves as "world-class public relations experts" to communicate risk, White said.

The life cycle of a terrorist plot can span from months to years, the presenters explained, with pre-attack planning ranging from intelligence gathering to surveillance, planning, rehearsal, and execution. At potential targets, site security can mitigate threats by practicing behavioral threat assessment, which requires identification of hostile intentions by, for example, being on the lookout for stress exhibited by people trying to conceal them.

The Mall of America uses a risk assessment and mitigation (RAM) methodology, also used by security for high-risk organizations and facilities in Israel, overseen by the mall's RAM unit.

**Intelligence.** We're all aware of the Internet's ubiquity in our daily lives. During a session titled "Best Methods for Using Internet Search Analysis in Intelligence and Investigations," former FBI special agent and investigator Edward J. Appel quantified its scope and offered expert tips on separating the wheat from the chaff online.

Appel, proprietor of iNameCheck, explained that 1.6 billion people worldwide use the Internet. (Some sources put it as high as 2 billion.) A total of 240 million Americans—80 percent of the country—is online. He classifies 30 percent of those Americans as "power users," who either access the Web via multiple devices or have an actual online presence, usually through social networking sites like LinkedIn or Facebook. Some use their real identities, and some remain anonymous.

"Almost 500 million people are using Facebook," Appel said. "Kind of scary. Not private."

Those online presences, along with other sources, provide a wealth of data for practitioners like personnel security professionals vetting potential hires. A simple search on the Internet will not cut it, however. Appel noted, for example, that he shares a name and age with another person elsewhere in the country who is married to a women with the same first name as his own wife.

So how can investigators ferret out valuable data? Appel acknowledged Google's great personal and recreational value, but he pointed out that it is a business predicated on selling ads by presenting users with links to popular pages that the company knows most users will want to see—not those with verifiable data."So, it's a very, very good tool to look for things, but it's not perfect, and it's not always going to give you exactly what you want to see."

A trove of practical sites—such as those containing information from government databases—is not even indexed by Google for presentation in search results. Among them are better-known sites like anywho.com and whitepages.com. Others provide more specialized data.

Whois.com offers information about the exact people controlling Web site domains. Nsopr.gov offers aggregated data about the nation's registered sex offenders. And SSNvalidator.com can tell users whether a Social Security number is in use or belonged to a person who is deceased.

On the data protection side, organizations must be extremely careful about what employees do on work computers, and what data they post online. Appel noted the new challenge that social networking sites pose to the U.S. Department of Defense. Pentagon leaders want service members to have robust communication with loved ones back home, but they don't want sensitive data available to potential enemies, he said.

**Public safety.** In "Video Quality in Public Safety from Research to Reality," presenters Carolyn Ford from the U.S. Department of Commerce, Joseph Gittens of the Security Industry Association (SIA), and Steve Surfaro of Axis Communications described the Video Quality in Public Safety Working Group, known as VQiPS, under the Public Safety Communications Research Program in the U.S. Department of Commerce. The group first met in February 2009, with the goal of helping arm public safety professionals with the information they need to find the right video surveillance equipment and improve the

ZVI KREMER makes a point about security profiling.

quality of the video they work with.

The VQiPS group is made up of various public safety practitioners, including law enforcement and manufacturers. Surfaro stressed the importance of image quality, which is essential to providing improved situational awareness during critical events.

Surfaro said that the working group is reaching out to the community. For example, the group plans to conduct surveys and develop a "recipe" of successes in various uses of video equipment. Surfaro asked public safety officials in the audience to assist in the effort.

CHIQUITA LEAK leads a panel discussion on leadership.

Some of the initiatives that VQiPS is undertaking include developing a user guide to help public safety agencies assess their video user needs and match those needs to technical specifications and standards, establishing a set of use classes, developing a glossary of common terms, creating an inventory of existing standards and specifications, and collecting a library of test clips that represent use classes and can be used by various agencies and users.

The project participants hope to put together best practices and system design specifications that can help public safety officers and others achieve the proper video quality to allow them to do their jobs.

Earlier this year, VQiPS released its first user guide. It was an initial framework, but does not yet include the various test results, which will be worked into a later release. The project aims to be a clearinghouse for existing standards, according to Ford.

Among the next steps are to put together specifications that address specific usage scenarios.

**Homeland security.** During a session called "Behavioral Pattern Recognition: A Proactive Approach to Homeland Security," veteran Israeli security consultant David Harel offered insight into how an individual's behavior, coupled with context, can highlight a threat of violence. Harel, worldwide managing director of ASERO Israel, refers to the approach as analysis of behavioral and contextual indicators.

The presentation featured a quote from Sigmund Freud, who said, "No mortal can keep a secret. If his lips are silent, he chatters with his fingertips; betrayal oozes out of him at every pore. And thus the task of making conscious the most hidden recesses of the mind is one which it is quite possible to accomplish." Translation, according to Harel: "I can read your body language."

There are many examples in which terrorists' behavior indicated the stress of the mission and efforts to conceal it. Harel listed the case of Abdulmutallab in which a screener at Amsterdam's Schiphol Airport reported a "gut feeling" to his supervisor that the attacker was acting oddly. The supervisor simply instructed the screener to put Abdulmutallab through the standard screening process, which failed to detect the explosive concealed in his clothing.

Harel's advice to security professionals looking for BHIs: Be a hunter, not a fisherman. Look for threats proactively and don't wait for them to present themselves.

**Data security.** In today's world of Internet-connected devices, clicking on the wrong link can lead to big financial and information losses, warned cyber-intrusion analyst David Morgan of Booz Allen Hamilton.

A prime example, Morgan said, is Washington, D.C., resident Nigel Parkinson. The owner of a successful construction company, Parkinson clicked on a malware-laced link in an e-mail last November. He thought the e-mail was from the Social Security Administration. He was wrong, and cyberthieves made off with $18,000 after the malware they installed recorded Parkinson's user name and password to his bank account.

Morgan said stories such as Parkinson's are commonplace, with hackers victimizing smart and well-defended companies and organizations like Google and the U.S. Department of Defense. These incidents will only increase as individuals and organizations fail to adequately protect themselves while continuing to hook up devices to the Internet. Consider this: this year an estimated 35 billion devices were connected to the Internet. By 2013, that number is estimated to exceed a trillion.

To drive the point home, Morgan asked how many people in the audience protected their smart phones with antivirus software, encryption, and passwords. Only a few raised their hands. His point was clear: cybercriminals have a lot of marks, and they are eager to exploit gaping vulnerabilities and victims ignorant of the threat.

Quoting various industry surveys and reports, Morgan told a tale of digital hor-



PHOTO BY OSCAR EINZIG PHOTOGRPAHPHY

ror. Eighty percent of intellectual property is stored digitally online. Only 4 percent of assessed and successful breaches used a sophisticated attack method. While 80 percent of companies restrict "unsupported" network devices, 40 percent of employees knowingly connected those banned devices to the company network. Security vendors can only detect 60 percent of malware at any given time.

If these statistics weren't bad enough, Morgan described cyberthieves as brilliant adversaries intent on stealing information and money. Every day, hackers create 19,000 vulnerabilities to break into networks. Worse, some hackers write software code to attack specific individuals and companies. Others manufacture code, like the Zeus botnet, and sell it to "nontechnical hackers," who use point and click interfaces to siphon funds out of victim bank accounts. Other malicious actors, on forums like GhostMarket.net, rent out their cybercriminal skills.

The answer to cyber insecurity, said Morgan, is multiple layers of security, such as antivirus, two-factor authentication, and firewalls, among other measures. Morgan, however, reminded the audience that there is no perfect solution and that vulnerabilities will always exist.

Morgan said companies should mandate security training and develop or strengthen computer-use policies. When employees violate those rules, there must be consequences. "Enforce the rules," Morgan stressed.

Victimized companies can also be good corporate citizens by sharing how they were attacked on forums, such as the public-private partnership known as the National Cyber-Forensics and Training Alliance. By doing so, victimized companies can help other businesses and individuals avoid those same mistakes.

**Investigations.** Social networking sites are playing an important role in investigations and lawsuits, according to speakers at a session titled "Seek and Ye Shall Be Sued: Using Social Networking Sites to Manage Risk without Risking Litigation."

It can be relatively easy to glean information about targets of an investigation or parties in a lawsuit, according to the speakers, especially if people have not made use of networking privacy settings. Data and photos available on networking sites can be useful in cases such as disability claims, cyber bullying, and domestic violence, they said.

Networking sites are becoming a much larger part of investigations and lawsuits partly because, in some cases, they can show what people have been doing "at any time," said Elizabeth Ho Sing, an associate at Wilson, Elser, Moskowitz, Edelman & Dicker.

It can be relatively easy to find and capture information on networking sites and blogs using screen video and picture capture tools, she said. In some cases, the investigator should first gather as much data as possible because it can be hard to know exactly what information could be useful. It can also be useful for investigators to try to capture a date on a Web page along with any posted data, she said.

During the session, a few speakers discussed cases in which people had made health disability claims against insurance companies. But evidence found on networking sites seemed to discount such claims and, therefore, weakened their claims.

People are often unaware that information is available about them online that could damage a case they are involved in, several presenters noted. In some cases, an attorney will ask a client whether there is information posted about them that could damage their case, but clients frequently underestimate the extent and availability of such information.

It can be more challenging and legally ambiguous to investigate networking information when users have made strong use of their privacy settings, the panel agreed. But investigators and attorneys do have tools available to them, including sending subpoenas to networking sites and asking defendants and other parties in a case about networking information during depositions. ■

**This information was drawn from editors' reports at the ASIS International 56th Annual Seminar and Exhibits. Don't miss next year's event in Orlando: Mark your calendar now for September 19-22.**