Published on *Security Management* (http://www.securitymanagement.com)

Inspiration and Instruction

By

More than 20,000 security professionals traveled to Orlando, Florida, in September to participate in the **ASIS International 51st Annual Seminar and Exhibits**. They sought inspiration and instruction. To help in the quest, an astounding array of 138 educational sessions was scheduled throughout the week. In addition, keynote headliners opened each day's general session, looking at the world of security and management from many angles. (For in-depth coverage of the full range of seminar offerings, including discussions of many of the products on display at the 2,470 booths, see November/December's ASIS Dynamics.)

ASIS Experiences Powell Power

You're a good leader when the troops will follow you, if only out of curiosity," said General Colin L. Powell (USA-Ret.) in his speech before a packed house during the **ASIS International 51st Annual Seminar and Exhibits**. Powell was greeted with cheers and a standing ovation at Tuesday's general session, where he spoke about being a good leader and lessons he learned as a young officer fresh out of Fort Benning.

"To accomplish a mission you have to take care of the troops, because plans don't accomplish anything, great ideas don't accomplish anything," Powell said. What is most important is people. "If you take care of the troops, you'll get the job done," a sergeant once explained to him ."Why? Because they trust you. They trust you because they believe in you and because you believe in them."

Powell related the lessons he learned about security in the military to the lessons that security professionals can learn from their experiences. Security needs to have a certain randomness to keep patterns from becoming predictable, he said, urging attendees to remember his infantry approach: defense in depth, active defense as well as passive defense, and "above all, deny the enemy any opportunity to perform reconnaissance against you."

Powell served the country for 40 years. He was National Security Advisor to President Ronald Reagan, a four-star general, Chairman of the Joint Chiefs of Staff, and ultimately the 65th Secretary of State.

He described the challenge of moving from Secretary of State, when he traveled in his own plane, to private civilian. Soon afterward, he took the Delta Shuttle from Washington, D.C., to New York and admitted to making three mistakes. "One, I showed up late. Two, I didn't have any luggage, and three, I paid cash."

As a result, he received close scrutiny from airport security, which drew laughs from the crowd. The screener even recognized Powell, leading him to wonder why he had been singled out.

The experience made it clear to Powell that while changes in airport security were certainly necessary after 9-11, the policies need to be reconsidered. He called America's openness its greatest strength. "If we are so tight that we cannot let commerce and traffic go in and out of our country, then we are the losers, and the terrorists are the winners."

Blanchard's Tips for Success

Making money is the happy side effect of running a great organization. This was the message that management guru Ken Blanchard, Ph.D., delivered to attendees at Wednesday's general session. According to Blanchard, organizations should strive to be the supplier of choice, the employer of choice, and the investment of choice. But if money is the only objective, he said, the entire company will suffer.

Blanchard is founder and chief executive of The Ken Blanchard Companies, an international training and development

company specializing in leadership, organizational change, and team building. He has authored more than 30 books, including The One Minute Manager, which has sold 17 million copies worldwide and has been translated into 25 languages.

Blanchard addressed relations between managers and employees. The path to good customer service—and increased sales—lies with frontline employees, he said. “Leaders must act like their employees have brains and can make decisions on their own,” Blanchard noted. “If you don’t give employees power, you will have poor customer service.”

Blanchard urged security leaders to decide what business they are in by developing a vision that is focused on the customer. “To compete, companies must have the right target,” he said. Blanchard pointed to Disney’s motto, noting that the company is in the “happiness business,” not the theme park business.

A Titanic Tale

The seminar and exhibits officially closed with a thrilling adventure as good as any found at Disney World. Robert Ballard, Ph.D., recounted his experiences as an undersea explorer most well known for his 1985 discovery of the HMS Titanic, the “unsinkable” luxury passenger ship that foundered after hitting an iceberg in 1912. Ballard and his exploits were featured in the television program Secrets of the Titanic.

Ballard has also tracked down other significant shipwrecks, including the German battleship Bismarck, the lost fleet of Guadalcanal, the U.S. aircraft carrier Yorktown, and the boat John F. Kennedy commanded, PT-109.

“I grew up wanting to be Captain Nemo from 20,000 Leagues Under the Sea,” he said. Today, Ballard is a National Geographic Society explorer-in-residence and president of the Institute for Exploration in Mystic, Connecticut. He previously spent 30 years at Woods Hole Oceanographic Institute and holds a Ph.D. in marine geology and geophysics from the University of Rhode Island, where he is a full-time faculty member.

Throughout his career, Ballard has conducted more than 100 deep-sea expeditions. A commander in the U.S. Naval Reserve, Ballard has published 18 books, numerous scientific papers, and a dozen articles in National Geographic.

Security Smarts

An impressive roster of session speakers covered myriad management and operational topics, capturing the latest thinking on major security issues. Sessions touched on specialty topics as well as on general security themes. One group of sessions evoked exchanges that challenged old paradigms, including those affecting emergency planning and management tactics.

Weathering storms. Hurricane Katrina would seem to have little to do with industrial espionage and competitive intelligence. Yet David Nicastro, CPP, underscored a critical component of both natural and manmade disasters: management must “realize how important it is to plan before a crisis hits.”

Nicastro, who had spent the previous ten days along the Gulf Coast helping people and businesses ravaged by Katrina, also noted that the loss of information assets often has a more devastating effect on businesses than the physical damage wreaked by the deadly hurricane.

Most of Nicastro’s presentation, however, focused on threats including wiretaps, social engineering, and computer intrusions, as well as on competitive intelligence ploys such as eavesdropping, the rental of office space adjacent to a target, and bribery. He noted that on a traditional threat matrix, industrial espionage often falls in the high-probability/high-consequence category.

The discussion frequently touched on examples of poor protection practices. One company that at first said it did not need protection came rushing back to Nicastro, a security consultant, after the company thought it had lost materials critical to its most important client. The material was found, and Nicastro took the occasion to perform a penetration test of the company. After two weeks of tailgating through doors and getting into computer systems, Nicastro had “pieced together $30 million of [the company’s] technological research.”

Nicastro concluded with an array of prevention strategies, including employee training, crisis-management planning, and reporting mechanisms. The best approach, he emphasized, is tiered layers of security.

Economic espionage. During his presentation, Frank Schurgers, managing director of Integris International, Ltd., made a claim that he knew would be unpopular. He said that although terrorism grabs headlines, it remains largely a concern

of the nation state and not of business.

Companies, he said, would be wiser to focus on economic crime as the primary drain to their bottom lines. And increasingly, these crimes can be linked to highly sophisticated and agile organized crime groups that have intimate knowledge of the international financial system. Companies fall prey to economic crime because of a number of issues, including complacency, ignorance of facts and warning signs, too much trust in business partners, and a "deep-seated denial of insiders as betrayers," said Schurgers.

Multinational corporations also fail to understand that the business "rules of engagement" are markedly different in some countries. To explain, Schurgers discussed a case he was involved in personally. Russian tax authorities unexpectedly audited a Russian company called Kosmotrade. The authorities spent an unusually long time inspecting the company's documentation but produced no final report.

Shortly thereafter, an armed robbery occurred at one of Kosmotrade's warehouses. It was a military-style operation during which three guards were wounded and about $1 million in goods was stolen.

Called to investigate the robbery, Schurgers' company found evidence that pointed toward a business partner of Kosmotrade—a distributor called Omega. Based on the findings, Kosmotrade severed its relationship with Omega.

The investigation could have stopped there, but Schurgers' company pushed it further, ultimately discovering that Kosmotrade was founded by former KBG officers as a KGB front. After the collapse of the Soviet Union, it became a genuine business, but was still operated by ex-KGB officers.

These "management executives" wanted to be rid of Omega as a middleman, and to do so set up the tax audit, planted disinformation, and staged the robbery to discredit its former business partner.

That type of scheme is not unusual in some parts of the world, said Schurgers, where the lines between businesses and authorities are not distinct and intimidation and pressure are a regular part of commerce. Schurgers suggested that the key to success was for a company to perform the best due diligence possible on its own employees and management, on business partners, and on business practices.

Global conflicts. Noted author and commentator Ralph Peters unleashed his own brand of sage advice on global conflicts during a Wednesday session. A retired U.S. Army officer with more than 20 years' service in assignments throughout the world, Peters left the military to write with greater freedom on events of the day.

Based on his experiences traveling to the four corners of the globe, Peters presented his views on the war on terrorism and global hotspots. He made projections on the outcome of the war in Iraq, saying that the delicate balance among the factions could tip either way in the near future. He scanned the political landscape in other Middle Eastern countries and voiced particular concern about Saudi Arabia.

Peters spent a good portion of the session discussing the future of Africa. While he acknowledged some sectors of the continent are under siege from war and disease, he was effusive in his praise for South Africa, which he felt was a model state with a healthy future.

Converging notions. The trade show floor in Orlando was replete with products such as networked DVRs and IP-based cameras that serve as evidence of how physical security and information security are moving closer together. But as the notion of converging the two departments becomes increasingly popular, businesses that attempt to do so are discovering problems that they never considered.

In a Tuesdsay morning session, Steve Hunt, CPP, CISSP, discussed some of the difficulties inherent in convergence and offered solid solutions to make the task easier. Hunt, president of consulting firm 4A International, discussed the "tangible objects and services" that cause convergence problems, including software, hardware, and locating and hiring professional services and consultants.

An even greater problem is what Hall called the "soft stuff," such as salaries, organizational charts, and policies.

Salaries are the most difficult of all, said Hall. Physical security professionals with decades of security, law enforcement, or military experience often get paid far less than IT security personnel, who may be just out of college. That can cause friction. Hunt recommended not putting the two groups in the same room even if they share the security label. Instead, the two groups should work together on projects with specific goals as a way to get to know and trust each other.

Problems in convergence, Hunt said, typically arise from two causes: executives who "just don't get it," and an inability by both physical and IT security professionals to articulate their goals.

For example, he said that, if asked, physical security members would say their goal is "to keep bad things from happening," while the IT team's goal would be "to permit business to continue uninterrupted."

Not only are these goals different, he continued, but they also are often at odds with each other. Therefore, said Hunt, security professionals must learn to communicate their value to executive management and form alliances.

Continuing the discussion on convergence, Chris Kelly, vice president at Booz Allen Hamilton, welcomed a standing-room-only crowd to a Thursday morning session on the topic. Kelly introduced the preliminary findings of a survey conducted by ASIS International, the International Systems Security Association, and the Information Systems Audit and Control Association. He noted that participants, predominately senior executives, agreed that convergence had become a major issue in all aspects of the business world.

While the participants were all in different stages of the convergence process, all agreed that convergence presents a major challenge with unprecedented potential. "We have an opportunity to see what the future has in store and how we can be prepared for it," said Kelly.

After Kelly's presentation, moderator Ray O'Hara, CPP, senior managing director with Vance, opened the floor for questions. Panelists Tim Williams, CPP, and Bill Boni, CPP, were asked what issue should be the driving force behind convergence. According to Williams, vice president of corporate and systems security with Nextel, regulatory compliance can be a change motivator. He added, "Security professionals in organizations that must meet these standards should embrace convergence as a way to prove their worth to the company."

Boni, vice president and information security officer with Motorola, Inc., urged attendees to inform senior executives of the critical value of information and company processes that depend on computerized components. "If a tangible product gets stolen, that is a bad thing," said Boni. "However, if someone sabotages an entire process, there is a major problem. The answer is convergence and taking a holistic view of security and company operations."

Security Technologies

Many sessions expanded current thinking on security technologies. While physical security topics were included in their own track, a discussion of applicable products permeated sessions on such far-flung subjects as mailroom security, computer forensics, and nursing homes.

A major component of the products on display at the 2,470 booths in the exhibit hall involved video in new and old permutations. The following summaries focused on using this security mainstay as well as emerging technology as evidence.

CCTV evidence. CCTV systems can yield evidence of criminal conduct that is admissible in court and can help make or break a case against the accused. Larry Brown, senior vice president, First Citizen's Bank & Trust Company, joined Richard Vorder Bruegge, Ph.D., examiner of questioned photographic evidence with the FBI, to show how to use CCTV properly in criminal cases. Vorder Bruegge laid out the Bureau's video guidelines that commercial institutions should follow to aid law enforcement in identifying people and objects in question.

"Lighting is critical," said Vorder Bruegge as he projected CCTV images that were useful as evidence as well as those that did not make the grade. Poor lighting is the most common factor degrading the quality of video images, he said.

He also pointed out other important factors in capturing clear images of suspects and objects of interest. Those mentioned included the number and placement of cameras, a bandwidth that is compatible with the system's resolution requirements, adequate electrical power, and physical security for the recorders.

Secure digital video. "I want you to leave this room with one thing and one thing only," said Brand Fortner, Ph.D., project manager at The Johns Hopkins University Applied Physics Laboratory. "Digital video needs to be secure."

Fortner and Postal Inspector Gregory Staisiunas, CPP, explained prototype software that they have developed to authenticate digital video from camcorders so that it can be used in court. The presenters riveted the crowd at the outset, showing a video montage of movies and television shows revealing how fantastic backgrounds such as skylines, rivers, and mountain landscapes were the result of digital wizardry. But because digital video can be manipulated easily, it's use as an evidentiary tool in courtrooms has been hampered, they pointed out.

Fortner discussed the various types of digital authentication currently available and a new approach being pioneered by Johns Hopkins, the U.S. Postal Inspection Service, and the Technical Support Working Group. (See “Intelligence,” page 22 for a discussion of the technology.)

Security Techniques

A group of sessions laid out research results, established laws, and government resources that can be used to enhance security programs and processes. The following descriptions highlight a few that were on the daily docket.

Master plans. Stephen Thompson, director of marketing, safety and security, Johnson Controls, detailed a research project completed by his company. To find better ways to build a budget and support for a safety and security plan, the company spoke to nearly 100 directors of such programs. The purpose was to find new ways to gain support for needed security.

As a result of the research, the company developed a security-needs prioritization method compiled through the participation of a client’s general and executive management, department heads, and users from different parts of the organization. During what Thompson called “distillation meetings,” participants are exposed to the basic safety and security functions in the company.

The meeting results in a needs-summary-and-prioritization report that visibly ties results to improvement projects and a long-range safety and security master plan. Because a cross-section of employees is involved, needed changes have a greater chance of buy-in from all sectors of the company.

Threat mitigation. Before a packed house, presenter Robert A. Cizmadia, CPP, lectured on how to use a Federal Emergency Management Agency (FEMA) reference that offers advice on mitigating threats against commercial buildings using design principles that include crime prevention through environmental design.

Called FEMA 426, the manual recommends an all-hazards approach, which makes an effort to protect against both environmental and terrorist threats. Cizmadia, who is senior project manager with PBS&J, said, “It’s very difficult to retrofit security,” encouraging the audience to make it a priority from design through building completion. The more influence security professionals have at the beginning of a construction project, the fewer problems they are likely to have once the building is in operation. “Our country has become complacent,” Cizmadia said, and security professionals must take on a much more proactive approach.

Information sharing. In the first of 33 sessions covering homeland security topics, three representatives from the Department of Homeland Security (DHS) discussed various programs within DHS geared toward public-private partnerships. Richard F. Williams, CPP, consultant to science and technology research and development, DHS; Thomas B. Taylor, chief, special programs division, DHS; and Steve MacKnight, operations manager, DHS/PCII Program Office formed the trio.

The speakers focused on the DHS Protected Critical Infrastructure Information program (PCII), which enables the private sector to voluntarily share sensitive information with government analysts. If the information satisfies the requirements of the 2002 Critical Infrastructure Information Act, it will be protected from public disclosure. The prohibition includes protection against disclosures initiated by Freedom of Information Act requests, state and local sunshine laws, and civil litigation.

MacKnight made several points about the program. First, he reminded the audience that 85 percent of the nation’s critical infrastructure is privately held. He emphasized that the PCII program will help DHS to work more efficiently with these companies since PCII ensures that only authorized and properly trained individuals will have access to a company’s sensitive information. In addition, the protection ensures that the information will only be used for the analysis of threats and vulnerabilities and other homeland security purposes. Finally, company information will only be disseminated to accredited government entities.

Antiterrorism model. During a Tuesday session, Jacqueline Rast, vice president and managing director of integrated security for CH2M HILL, presented several case studies featuring the use of AT-MAP. The method is a government project that combines physical facility surveys, U.S. Department of Defense (DoD) antiterrorism standards, and geographic information system technology to assess and make decisions about where to invest in antiterrorism improvements.

AT-MAP was originally created to help installations comply with reporting requirements. As the program was

developed, management tools that help Air Force staff make wise fiscal decisions were incorporated.

The basic functions of AT-MAP allow for the analysis of an installation's antiterrorism status as it relates to DoD standards and provide details on where upgrades and changes should be made. In addition, the project has established a common language among the engineers, security officers, and planners that need to coordinate compliance with antiterrorism standards.

Installing this method and coordinating response takes time before it can run smoothly, said Rast. For that reason she recommended that any emergency response efforts be practiced and tested long before an event might occur.

Assessing risk. Creating a comprehensive antiterrorism plan requires an astute awareness of likely risks and vulnerabilities. Detection, which includes input by both human and technological devices, is the first step to a good protection plan, according to Victor Vella, senior antiterrorism specialist with the DoD. Once a risk has been detected, it must be assessed and evaluated to determine the proper response, he said.

Drawing on his experiences dealing with terrorist incidents such as the Oklahoma City bombing, Vella detailed the Risk Analysis Vulnerability Assessment (RAVA) methodology used by the federal government to assess risks. The RAVA analysis uses mathematical equations that are generated from a questionnaire, which produces a quantitative measurement of the threat, the target, the vulnerability, and the risk.

Each question associated with the questionnaire is weighted as to its significance in countering a specific threat. Questions such as, "Have there been any terrorist attacks on similar assets?" and "Are there any business interests from terrorist watch list countries in the area?" paint a clear picture of the entire security situation.

According to Vella, "We simply cannot afford comprehensive protection," so intensive vulnerability assessments, like RAVA, are integral to fighting terror.

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals, with more than 37,000 members worldwide.

ASIS International, Inc. Worldwide Headquarters, 1625 Prince Street, Alexandria, Virginia 22314-2818 U.S.A.
703-519-6200 | fax 703-519-6299 | www.asisonline.org

Source URL: http://www.securitymanagement.com/article/inspiration-and-instruction