SECURITY MANAGEMENT
SECURITY'S WEB CONNECTION

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

Attendees Gain Insight at Intensives

Those attendees seeking extra information or insight into specific security topics arrived early in Anaheim to attend various preseminar intensives—courses presented by experts on topics ranging from consulting to securing houses of worship. The intensives were held at the Anaheim Marriott adjacent to the AnaheimConvention Center on Saturday and Sunday before the launch of the ASIS International 55th Annual Seminar and Exhibits. The programs covered issues such as security consulting, managing in a crisis, security assessments, securing the corporate network, critical infrastructure protection, securing houses of worship, and hotel crisis response.

SECURITY CONSULTING

On the opening day of the "Successful Security Consulting" intensive, Richard Grassie, CPP, managing principal of Good Harbor Consulting, LLC, in Rockland, Massachusetts, told attendees that running a security consulting business can be rewarding. However, he warned that starting a business can be very tough in the beginning. "Stay focused and stay in the business," he said. "The key is to have tenacity and to package your consulting company properly."

Grassie, along with fellow presenter Frank Pisciotta, president of Business Protection Specialists, Inc., in Raleigh, North Carolina, outlined both the good and bad aspects of starting a security consulting practice. Among the good features, Grassie told attendees, are being your own boss, using your skills and knowledge in a variety of ways, and working on a range of projects in numerous locations. However, balancing the scales are the excessive travel, competing against low bids, and facing down clients who refuse to pay their bills.

Attendees also learned to assess the competition. According to Grassie, many people who entered the security consulting business after 9-11 were not fully qualified. It is especially important, he noted, for legitimate security professionals to be aware of these operations and stress their competence and certifications. One way to determine whether unqualified companies are bidding on a job is to assess the range of bids. "On one job we won, the range of bids was from $20,000 to $150,000," said Grassie. "We knew that no one could do the job well on the cheap end of the scale and that those high-bidders did not know what they were doing."

Other topics covered in the two-day course included marketing a consulting service, developing an online presence, writing a business plan, viewing the business from an end-user perspective, and keeping abreast of consulting trends.

HOTEL SECURITY

On Sunday morning, attendees gathered to hear the latest on security in the hospitality industry at "Hotel Crisis Response and Tabletop Exercise." Led by Skip Brandt, CPP, of the ASIS Hospitality, Entertainment, and Tourism Council, the session took the form of a tabletop exercise designed to confront an active-shooter crisis at a hotel. The results of the exercise informed fresh insights into handling crises at hospitality operations and included discussion and critique of the hypothetical crisis.

Brandt told attendees that his definition of a crisis "is anything that disrupts guest services." For example, the Boston hotel at which he is the security director is more than 80 years old and has suffered regular water leaks and major waterline breaks, one of which sent more than 22,000 gallons cascading through the accounting department's server room. How to act in these situations is a prominent part of that hotel's crisis management plan, and the hotel has invested in sump pumps and other equipment to provide a speedy reaction. In the case of the flooded server room, Brandt said that the waterline break occurred at 7:30 a.m. and by 9:30 a.m. "the accounting department was back in business."

The scenario that Brandt laid out in the tabletop exercise took place in 1,200-room hotel just after midnight when few employees were on duty. Those who were included a handful of bartenders and food servers, a few housekeeping employees, some engineers, a bellman, and three security officers. “In the middle of the night, this tiny staff is typical at a hotel,” Brandt said, and the quandary for the first part of the exercise was how to best deploy these few workers and just what they could reasonably be expected to do during the crises.

In this case, a guest called the front desk to report loud arguing in a room nearby. The two security officers who responded heard more angry voices and what sounded like shots. Among the interesting points brought up for consideration was that while security officers are often sent to investigate reports of what appears to be domestic violence, the vast majority of hotel security officers—unless they are off-duty police officers—are probably not familiar with the sounds of gunfire. Because they are unsure, they sometimes hesitate in contacting police. “They’re sometimes afraid of embarrassment if they are wrong, knowing that calling in gunshots will bring a heavy police response.”

As the crisis progressed, the security officers saw a man leave the room with a weapon in hand and head into a stairwell. A woman who had been shot and appeared to be close to death was found in the room. Attendees at the session then spent the remainder of the day discussing the minutia of how each employee present in the hotel could best react. Other issues included employee interaction with police and EMS personnel, ways to preserve the crime scene, logging the event, notifying guests to remain in their rooms or telling them when they should try to evacuate, and using the CCTV system to the greatest advantage. In the case of CCTV, among the points noted was that it is best to have a trained officer remain at the security control room, as opposed to bringing in someone such as an engineer who has been trained to handle some security operations. The officer could then use the CCTV system to the best advantage and also appropriately log the actions of the crisis. It was also noted that it is vital that the security operations center have hands-free telephone receivers so that the officer can stay on the line with police or other responders, as well as manipulate CCTV cameras and keep a log.

MANAGING IN A CRISIS

The recent firefight at the United StatesHolocaustMemorialMuseum in June proves that well-trained security guards are a vital component to any security program, according to a presenter during the preseminar intensives yesterday.
Stevan P. Layne, CPP, of Layne Consultants International, argued that the shooting could have been “a lot worse” if two security guards present didn’t have the appropriate training to take down the alleged suspect, 88-year-old James W. von Brunn, a white supremacist. After von Brunn fatally wounded security guard Stephen Tyrone Johns at the entrance, the security guards and the rifle-wielding von Brunn began shooting at each other. The security guards hit von Bronn twice, wounding him. Von Brunn is currently awaiting trial, charged with murder.

Layne took a controversial stance during the preseminar intensive devoted to staffing levels in a down economy, arguing no amount of technology can replace live humans in certain security positions. Layne was absolute in his professional opinion that a human being must be present at certain locations in a facility, especially the main entrance. They need not be guards, he said, offering a receptionist as a suitable alternative, but there should be someone present at the main entrance that can make a split-second decision to call police or emergency personnel if the situation warrants it.
Layne also told attendees that security managers set higher professional and physical standards for their guards. At cultural locations, like the HolocaustMuseum, guards should have to undergo classroom training to ensure they understand their responsibilities. On the opposite spectrum, guards should have to be physically fit enough to perform their job. Layne said front-line guards should be able to lift a 50-pound fire extinguisher, carry a small child to safety, and remain on their feet for an entire eight-hour shift.

Another smart business decision security managers should make second nature is monitoring their guards, especially when it comes to incident reports. Guards need training to ensure they can write readable incident reports and managers should review the reports as frequently as possible. Good incident reporting will ensure that security managers can justify their budgets to management and show a return on investment when the time comes.
Security managers, finally, should educate their entire organization about the value of security and how their awareness can make security personnel’s jobs easier and the organization safer as a whole, Layne said.

CRITICAL INFRASTRUCTURE

The U.S. Department of Homeland Security's (DHS) infrastructure protection division, which helps spot vulnerabilities in critical infrastructure and key resources (CI/KR), is now looking at the issue regionally and considering the cascading effects of attacks on critical links, a senior agency official said Sunday.

John Walsh, CPP, supervisory protective security advisor (SPA) for the Great Lakes Region with DHS's Office of Infrastructure Protection (OIP), was one of several expert speakers at the preseminar intensive session titled "Critical Infrastructure Protection: An Educational Forum."

OIP was conceived in the months after 9-11, but its role came to the fore in 2004 after an al Qaeda notebook computer, discovered overseas by U.S. forces, was found to contain detailed schematics and casing data about major financial institutions in New York City and New Jersey.

At least one SPA is assigned to each U.S. state, and they work closely with state and private sector authorities to analyze vulnerabilities at sites that one former DHS official called "the crown jewels" of national CI/KR. During OIP site assistance visits, experts in red teaming spot potential vulnerabilities and provide owner operators a set of options for shoring them up. Implementation by owner operators, however, is entirely voluntary.

Disasters like the 2007 collapse of the I-35W bridge in Minneapolis highlighted the interdependency of CI/KR elements. Now, both in simulations and following actual incidents, OIP maps interdependency to determine which assets bear greater security risks based on the degree to which other functions rely on them.

OIP provides vulnerability analysis software to owner operators that they can use to create a "dashboard" of vulnerability ratings for different assets. Those ratings can be combined to assess mitigation across regions or the country, Walsh said.

Later, attendees heard from Rick Dinse, former chief of the Salt Lake City (Utah) Police Department and now law enforcement advisor to Federal Emergency Management Agency (FEMA) Administrator Craig Fugate. Dinse discussed evolving efforts to ensure law and order following a disaster on the scale of Hurricane Katrina, in which local agencies themselves fragment or dissolve altogether.

The federal government's post-Katrina solution was to develop law enforcement deployment teams, which would activate after a disaster and deploy to work under the designated incident commander. The method, however, has proven prohibitively expensive, and Fugate is looking to states and locals for a similar alternative. Under a current FEMA plan, "strike teams" of 12-70 volunteer state and local law enforcement officers would deploy to affected areas, with 75 percent of personnel costs covered by the federal government in national-level disasters, Dinse said.

FACILITY SECURITY

Seminar attendees received an in-depth look at developing effective security programs at Sunday's preseminar intensive "Facility Security Assessment and Initial Conceptual Design," presented by the ASIS Security Architecture and Engineering Council.

The intensive was led by Hunter R. Burkall, PSP, security consultant with Aegis Security Design, Inc.; W. Douglas Fitzgerald, CPP, director of security and technology at Vitetta/Fitzgerald; and Richard P. Grassie, CPP, managing principal of Good Harbor Consulting, LLC. The speakers said that some of the common problems with security programs are a lack of planning and resources and a poor design concept.

One of the integral components to a successful security program is to differentiate security threat from risk, said Grassie. A threat is any event or circumstance that can cause harm to the organization, while a risk is the likelihood that a threat agent will successfully mount an attack.

Grassie explained that a successful building design project consists of a core team of architects, engineers, and security consultants. It's integral that security be consulted at the start of the project. Grassie said that architects and engineers are becoming more accustomed to security being a major part of the design. Architects should also work within a "design basis threat," which is a profile of potential adversaries and their capabilities. This allows the architects to know which potential security scenarios to design for.

Burkall stressed how important it is to gather information from a variety of stakeholders when conducting security assessments. For example, if Burkall were assessing a hotel, he would speak not only to staffers in security, landscaping, and facilities, but to housekeeping and anyone loitering outside the hotel who might provide a unique perspective on how to get in or how secure the building is.

The speakers highlighted examples of how a successful security assessment can deter attackers. Burkall cited the three hotels in Amman, Jordan, that were bombed by terrorists in November 2005. Burkall said Marriott International had recently had an international loss prevention group conduct risk assessments at its Amman hotel and determined that it needed to increase security. Marriott might have been a primary terror target, Burkall says, if the hotel had not increased security, transfering the risk elsewhere.

SECURING HOUSES OF WORSHIP

While high-profile attacks on churches, mosques, and synagogues in recent years have slightly increased public awareness of security issues in houses of worship, ASIS security professionals are striving to improve security programs in faith-based organizations through awareness and education.

Presenters at the preseminar event “Securing Houses of Worship” discussed the behind-the-scenes efforts to raise the profile of security for faith-based organizations within the Society. These efforts have resulted in the House of Worship Working Group and the subcommittee on faith-based organizational security located within the Museum, Library, and Cultural Properties Council.

Jeff Hawkins, executive director of the Christian Security Network and vice chairman of the Museum, Library, and Cultural Properties Council, said that in setting up the subcommittee, the goal was not to be just a group of Christian organizations alone. “We need input from everyone,” Hawkins told participants. The goals of the new subcommittee are to establish guidelines on how to secure houses of worship as well as best practices for faith-based organizations.

One challenge for those hoping to protect religious organizations, however, is building a case for security. Convincing churches that they need to put a security program in place is a problem, Hawkins said. Security professionals are accustomed to building a case for security in the corporate world, but faith-based organizations sometimes present a unique argument against having a formal security program: they should entrust security to their god. “Before you can even talk about security you are in a religious debate with pastors,” he said.

Other organizations worry about “fortress-like” security programs and fear they will be perceived as uninviting. Hawkins said the key is to tell church leaders that “security” means being free from fear; it does not mean “guards, guns, and metal detectors.”

Hawkins noted that houses of worship are often soft targets, because they have no formal security program, and are seen as passive because they often do not press charges if they are targeted.

Hawkins cited Christian Security Network research, saying churches experienced more than 700 security incidents in 2009 thus far. The group estimates churches suffered $25 million in losses from security incidents in 2009.

Scott Watson, CPP, CFE, security manager at IDEXX Laboratories, emphasized that faith-based organizations experience the same kinds of security concerns as elsewhere. “If it happens in every other aspect of society, it can happen in a house of worship,” he said. Incidents might include active shooter situations, financial fraud, sexual misconduct, litigation, or simple medical emergencies. Watson stressed the importance of a risk analysis and instructed participants on a methodology.

Other speakers at the session included Nawar Shora, legal director and head of diversity education and law enforcement outreach at the American Arab Anti-Discrimination Committee, who discussed ways to facilitate the public-private partnership with law enforcement, and Chris Delia, director of security for the Anti-Defamation League, who focused on background screening.

CONVERGENCE

Converging physical and information technology (IT) security can be a way to boost security and cut costs. An increasing number of organizations are implementing Internet Protocol-enabled video or adding devices, such as printers, to employee access systems.

Before implementation, however, IT and physical security managers should work closely to ensure that such projects meet broader governance, compliance, and other goals, according to several speakers at a recent preseminar intensive.

By better understanding physical security's polices and business objectives, IT managers are more likely to gain backing for a project, said James Connor, a principal at Santa Clara, California-based N2N Secure, a security consulting firm that specializes in convergence. Such knowledge can also make it easier to build a business case for a project, said Connor, speaking at the preseminar intensive "Safely Putting Your Security Systems onto the Corporate Network."
Many physical security departments have written policies on certain security areas, Connor said. An example could be access control; primary objectives could be improving security and gaining a better audit trail. IT managers could help explain how a project meets such objectives, he said.

IT and physical security frequently have maps or outlines showing how networks and systems, for example, should be configured to comply with regulations.

Comments

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

Powered by: Phase2 Technology

Source URL: http://www.securitymanagement.com/attendees-gain-insight-intensives