THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 8 NUMBER 6

DECEMBER 2009

COMMERCIAL FACILITIES

Contact: CIPP02@gmu.edu
703.993.4840

In this issue of *The CIP Report*, we highlight the Commercial Facilities Sector. This Sector, which includes facilities such as shopping malls, stadiums, and self-storage services, is vital to protecting this Nation's critical infrastructure.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION

The first article, written by the Commercial Facilities Branch Chief, provides an overview of the Commercial Facilities Sector. The second article, submitted by researchers from the Manhattan College and University of Pennsylvania, analyzes the risks associated with shopping in an age of terrorism. This analysis is followed by an article by the RAND Corporation that assesses the options available to protect shopping malls from acts of terrorism. The Institute of Security Studies at the University of Nevada at Las Vegas then discusses their research regarding the improvement of the relationship between the Commercial Facilities Sector and Intelligence Fusion Centers. Next, the Self Storage Association provides two articles on self storage security. The first article discusses the potential security threats to self storage facilities. The second article discusses the role of the self storage facility operators. The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, then provides information about their operation of the Building and Fire Research Laboratory (BFRL). The National Center for Spectator Sports Safety and Security (NCS4), located at the University of Southern Mississippi, addresses the safety and security of sporting events. Next, we include an interview with an architect and security expert from the state of New York. Then, we feature an article, which includes input from a loss control services specialist with the Chubb Group of Insurance Companies, about insurance available to commercial facilities. The Director of Public Relations for Mall of America describes the extensive security measures that are in place at the Mall of America to protect its millions of visitors during the regular and holiday shopping seasons.

This month's *Legal Insights* examines the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act).

Finally, we are pleased to recognize President Obama's designation of December as Infrastructure Protection Month. This proclamation serves as a pledge to preserve the critical infrastructure of the United States.

We would like to take this opportunity to thank the contributors to this month's issue. We truly appreciate your valuable insights.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP
George Mason University, School of Law

Securing the Commercial Facilities Sector: It Starts With People

by Dave Crafton, Commercial Facilities Branch Chief
Sector-Specific Agency Executive Management Office
DHS Office of Infrastructure Protection

When families are prepared — when communities stand together and stand tall — so does our nation. United, we send a powerful message to those that seek to do us harm: we cannot be broken, we are America — strong and resilient. – U.S. Department of Homeland Security Secretary Janet Napolitano, September 29, 2009

Protecting the Nation's critical infrastructure is essential to making America safer, more secure, and more resilient. Within the unique and voluntary sector partnership framework established by the National Infrastructure Protection Plan, the Commercial Facilities Sector, with its vast array of public and private sector partners, is working hard every day to improve its ability to respond to and recover from the effects of natural disasters and manmade events, such as terrorist attacks. Considering the diversity of the Commercial Facilities Sector, this is a formidable challenge.

The Commercial Facilities Sector contains an array of mostly privately owned facilities where large numbers of people congregate, and where owners and operators must strike a delicate but appropriate balance between the principle of open public access and security. That challenge rests in maintaining a secure, resilient, and profitable sector in which effective and non-obstructive risk management programs instill a positive sense of safety and security in the public and sustain favorable business environments conducive to attracting and retaining employees, tenants, and customers.

Employees. Tenants. Customers. At its core, this is what the Commercial Facilities Sector is about — its people. Each individual within the sector, whether employee, tenant, or customer, carries with them a responsibility to promote the general security of those around them. When all Americans have an improved awareness of the necessity of infrastructure protection, our Nation is more prepared and resilient.

Public and Private Partnership for Critical Infrastructure Protection

Within the U.S. Department of Homeland Security's (DHS) Office of Infrastructure Protection, the Commercial Facilities Sector-Specific Agency (SSA) facilitates this sector partnership framework by working closely with public and private sector partners to collaboratively resolve security issues and address threats to the sector. The Commercial Facilities Sector is composed of eight diverse subsectors, each with its own set of needs and challenges. As a result, the SSA must respond to the diverse and changing security and preparedness needs within each of the following eight subsectors:

1. **Entertainment and Media** (e.g., motion picture studios, broadcast and print media);
2. **Lodging** (e.g., hotels, motels, conference centers);
3. **Outdoor Events** (e.g., theme and amusement parks, fairs, campgrounds, parades);
4. **Public Assembly** (e.g., arenas, stadiums, convention centers, performing arts centers, aquariums, zoos, cultural properties);
5. **Real Estate** (e.g., office and apartment buildings, condominiums, self-storage);
6. **Gaming Facilities** (e.g., casinos);
7. **Retail** (e.g., retail centers and districts, shopping malls); and
8. **Sports Leagues** (e.g., professional sports leagues and federations).

In addition, the Commercial Facilities SSA coordinates with other DHS entities and other Federal agencies to make their resources and tools available to sector partners and to develop new tools and resources to meet the ever-evolving needs of this sector. All of these efforts are insignificant without their implementation at the owner/operator level. By developing, implementing, and

(Continued on Page 23)

Shopping in an Age of Terrorism: Consumers Weigh the Risks Associated with Online Versus In-Store Purchases

by Carolyn E. Predmore, Janet Rovenpor and Alfred R. Manduley, Manhattan College
Tara Radin, Wharton School of Business, University of Pennsylvania

Up until the late 1990s, consumers had come to expect physical and financial safety when they went out to purchase goods or services in familiar neighborhoods. Their sense of well-being, however, was shattered by the terrorist attacks on the World Trade Center in 2001 and by the sniper attacks on residents in the Washington, D.C. area in 2002. Airplanes flying into the Twin Towers destroyed the offices of over 430 businesses from 26 countries as well as 500,000 square feet of retail space housing 75 stores, restaurants, and service outlets. The month-long killing spree of a pair of snipers in the D.C. area occurred at the onset of the winter holiday season and threatened the sales of all stores and restaurants.

Shoppers, commuters, and tourists have experienced similar acts of violence in cities all over the world. In 2003, 42 people, including 13 suicide bombers, were killed in explosions at five separate sites in Casablanca, Morocco. In 2003, two powerful bombs concealed in parked taxis killed 50 people and wounded 129 in the heart of Bombay, India. In 2004, bombings killed 191 people riding commuter trains on the railroad system in Madrid. In 2005, 56 people died and over 700 people were injured in attacks on three subway trains and a double-decker bus in London. These horrifying events, unfolding in the midst of major cities and surrounding suburbs, instill fear in ordinary citizens, which could force them to consider if or how they might change the way they commute to work, run errands, shop for groceries, and attend social gatherings. Analysts at BizRate.com, for example, reported that online sales increased 17% above normal levels in the weeks following September 11. It was suggested that the feelings of fear people had about going to public places might negate concerns over fraud and privacy often associated with shopping online.[1]

Consumer Perceptions of the Risks Related to Shopping

According to the Federal Bureau of Investigation, 4,000 threats — some credible and some not — were made against malls and shopping centers in the United States between 2001 and 2004. Malls made the list of most likely terrorism targets because they "represent Western materialism" and draw "large groups of unsuspecting shoppers."[2] Our research sought to answer the following question: Does violence or the threat of violence in the retail arena lead to more usage of online retailing? We chose to study the attitudes of U.S. consumers for whom acts of terrorism are a relatively recent threat and Israeli consumers who have faced physical harm and disruption to daily routines for many years.

In a survey, we collected consumer opinions on safety and security in an online shopping environment as well as in a typical shopping center format in two countries: the United States and Israel. Our research builds upon the Bhatnagar and Ghose model by considering different types of risks associated with shopping.[3] We wanted to determine if the decision to shop in person or online or to use a combination of other shopping techniques — catalog or telemarketing — depended on the amount of perceived risk deemed to be inherent in the shopping/purchasing experience and the total amount of perceived risk the consumer is willing to assume. Six

(Continued on Page 4)

[1] Rubin, Elaine and Ann Fairhurst. (2001). Fear of terrorism will draw more consumers to buy online. *Electronic Commerce News*, 6(41) 1.
[2] Ethridge, Mary. (2004). Malls make list of most likely terror targets. *Knight Ridder Tribune Business News*, June 19, 1.
[3] Bhatnager, Amit and Sanjoy Ghose. (2004). Segmenting consumers based on the benefits of internet shopping. *Journal of Business Research*, 57 (12), 1352-1360.

Consumer Risks *(Cont. from 3)*

types of perceived risk — functional, physical, financial, social, psychological, and time — were identified in the consumer behavior literature.[4] The amount of the total perceived risk might be a constant while the levels of the types of perceived risk varied with the elements of the situation:

Total Perceived risk = Summation of risk = Evaluations of functional + physical + financial+ social+ psychological + time.

Rather than specify the types of risk attached to the Internet buying experience, it seemed likely that an individual might be operating with many forms of risk. A consumer who attaches high financial risk to shopping online may typically elect to shop in person at "bricks and mortar" stores.[5] He may, however, be forced to re-evaluate his shopping patterns if there is an increase in the physical risk involved in shopping in person. Instead of admitting his fears, he might justify his decision to shop online because it saves time (resulting in low perceived time risk). Another consumer might perceive social risk in avoiding a mall and missing out on an enjoyable time with friends. She would venture out to the meeting place despite the perceived physical risk. Psychological risk can occur when the consumer believes that the violence is dictating how he runs his life.

In this study, we focused primarily on financial, functional, physical, and social risks associated with the decision to shop online versus the decision to visit a "bricks and mortar" store. We examined shopping behaviors using a self-report survey given to 329 men and 312 women between the ages of 14 and 86 (with an average age of 24) in the U.S. Household income ranged from less than $25,000 per year to over $100,000 per year.

The Israeli survey was administered to 50 respondents. They were given virtually the same survey as the U.S. respondents except that it was in Hebrew and household income was reported in shekels rather than dollars. The average age of the Israeli respondents was 40 years with a range from 19 to 75. There were 17 male and 33 female respondents.

Results of a Study on Terrorism and Shopping

Results from our survey revealed that men and women in the United States weighed the risks regarding their choice of where to shop, differently. Women favored buying online when concerned with physical safety while men did not seem to be concerned or did not voice concern about physical safety in a shopping center or mall (Chi square = 15.0558, p = .006). Men in the United States were more worried about the possibilities of identity theft and financial fraud online than women (Chi square = 7.1556, p = .0002).

In general, Israeli women were not interested at all in shopping online. They reported functional risk with the buying of large and expensive items such as furniture. They felt that these items needed to be personally inspected before making a purchase. Israeli women did prefer shopping on a few international sites, like eBay, when the country was on a high security alert. These were considered to be safer alternatives to shopping in person. Israeli men, in contrast, did not show a preference for shopping on international websites compared to physical stores (Chi square = 10.4694, p=0.026). Once again, gender differences regarding which risks are more salient for men versus women emerged.

Israelis have continued to desire shared personal social interaction in shopping areas and malls. Israeli social norms for using shopping as a social experience appear to have more importance in the face of continued violence than does buying online which offers greater physical safety but is more socially isolating. This finding supports the research comparing Korean consumers with American consumers. Societies, which have traditionally put a premium on the social collective, may be slower to use the Internet for e-commerce.

(Continued on Page 24)

[4] Evans, Joel and Barry Berman. (2005). Chapter 8 – final consumers. *Marketing, 9e: Marketing in the 21st Century*, Atomic Dog, Cincinnati, OH, 216.

[5] Kimery, Kathryn M. and Mary McCord. (2002). Third-party assurances: mapping the road to trust in e-retailing. *JITTA: Journal of Information Technology Theory and Application*, 4(2), 63-80.

Protecting Shopping Malls

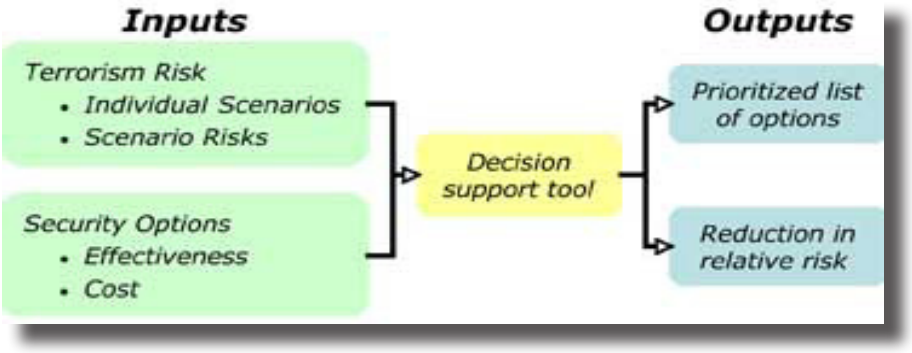
by Tom LaTourrette, David R. Howell, David E. Mosher, and John MacDonald
RAND Corporation

The threat of terrorism at commercial shopping centers is a prominent concern, with over 60 terrorist attacks against shopping centers in 21 countries from 1998 to 2005. Within the United States, shopping centers have been identified as potential terrorist targets, with specific warnings about attack threats at shopping centers in Los Angeles in April 2004 and again in Columbus, Ohio, in June 2004. While no attacks occurred in either case, the warnings led to widespread panic and disruption. In response to this potential threat, shopping center operators are beginning to explore and implement increased security efforts specifically designed to combat terrorism. In order to assess options for reducing the risk of terrorist attacks in shopping centers, we have used a modeling approach to help shopping center operators evaluate candidate security options in terms of their effectiveness at reducing terrorism risk.[1]

Our modeling approach uses the same logic that is used for planning security for more common security hazards: analyze incident frequencies and consequences and design security efforts to target the highest risk hazards. The difficulty, of course, is that terrorism risk is less familiar and far more uncertain than more common hazards like theft, workers' compensation, or injury liability. This requires using a systematic approach to characterizing risk and risk reduction.

The basic approach involves incrementally reducing the risk from terrorism by sequentially implementing security options. The options are ranked based on their effectiveness at reducing risk and their cost. The elements of the model are a set of 17 attack scenarios, estimates of the relative likelihoods and the consequences (casualties and property damage) of each scenario, a set of 39 potential security options, the cost of each option, and the likely effectiveness (expressed in terms of deterrence, denial, and mitigation) of each option in each scenario. Scenarios include various types of placed, suicide, and vehicle bomb attacks, armed assaults and hostage situations, and chemical and biological releases. Security options span a range of approaches, including communication and education, emergency response, employee management, entrance management, building management, vehicle management, and chem/bio management. Model inputs are drawn from multiple sources, including an analysis of terrorist attack statistics in shopping centers and in general throughout the world, case studies of individual shopping centers, security and crime deterrence literature, and information from technology suppliers. For a given risk outlook, the model provides a prioritized list of security options, the cumulative decrease in relative risk, and the cumulative cost as each option is implemented. The general model architecture is shown in the figure.

(Continued on Page 6)



[1] This article is based on the report, *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options*, by LaTourrette T, Howell DR, Mosher DE, and MacDonald J, 2006, RAND TR-401, http://www.rand.org/pubs/technical_reports/TR401/.

Protecting Malls *(Cont. from 5)*

We applied our model to three specific shopping centers in the United States: an outdoor shopping center with underground parking, a large indoor center surrounded by surface parking, and an urban center at which many customers enter from the street and from public transportation. The specific centers span a range of important shopping center characteristics, such as size, parking arrangements, indoor versus outdoor, and urban versus suburban. Despite important differences in design characteristics among the centers we examined, the modeling results for the different centers are very similar (8 of the top 10 options for each of the three centers are the same and few options are shifted by more than two positions among the three centers). As a result, some important general conclusions about terrorism security at commercial shopping centers can be drawn from our analysis:

- Based on our model and assumptions, implementing the security options considered in this study could reduce the risk of terrorism at malls by a factor of 20.

- Nearly all of the modeled risk reduction would be accomplished with the 6-10 highest priority security options.

- These high-priority options span a diverse range of approaches, including communication and education, emergency response, customer entrance management, vehicle management, and building management.

- As with terrorism at other target types, the primary terrorist risk at shopping malls is from placed bombs. Consequently, the prioritization of security measures is dominated by bomb risk.

- The three highest priority security options are encouraging mall patrons to immediately report unattended bags, placing bollards at pedestrian entrances to block suicide car bombers from entering the mall, and searching common area carts and kiosks daily for devices or weapons.

- Most risk reduction occurs with less expensive options; the average cost of each of the highest priority options is 20–35 percent of the average cost of all the options considered.

- The overall annual cost of the highest priority options ranges from $0.4 million to $2.0 million at the three centers examined.

- Typical disaster preparedness plans provide little benefit for reducing terrorism risk. In most cases, little can be done to reduce consequences of a terrorist attack once it has occurred (e.g., a bombing). Disaster preparedness plans and exercises, however, focus primarily on the emergency response and thus offer little toward reducing the risk of terrorism.

In conjunction with the quantitative model, we also included qualitative assessments of some of the collateral (i.e., non-terrorism-related) benefits and detriments of each security option. These collateral effects were most commonly negative (e.g., impeding customer access, inconveniencing employees, or negative psychological impacts), though several options could aid loss prevention or help reduce workplace violence as well. These collateral effects are very important in influencing decisions about implementing security options, but are presently too poorly understood to quantify in a model such as this.

Our analysis shows that, despite great uncertainties, using a rational, systematic approach distinguishes security options in ways that might not be intuitively obvious. It is important to point out, however, that decisions about when to implement security options will depend on perceptions of the absolute risk of terrorism. This analysis provides useful guidance about prioritizing security options to reduce terrorism risk, but it does not address the overall risk of terrorism. Despite the best analytical efforts, the evolution of this perception is likely to be complex and guided by indirect indicators, such as government actions and guidance, political changes, press coverage, or industry trends. It is therefore difficult to

(Continued on Page 32)

Supporting the Information Sharing Environment: Improving Liaison between the Commercial Facilities Sector and Intelligence Fusion Centers

by Robert J. Coullahan, CEM, CPP, CBCP, Nancy E. Brune, Ph.D. and Ross Bryant, PMP*

The Institute of Security Studies (ISS), at the University of Nevada at Las Vegas (UNLV), is actively contributing to an enhanced information sharing environment (ISE), and strengthening criminal justice and emergency responder strategies for preventing and mitigating terrorist incidents in the Commercial Facilities Sector (CFS) — particularly the hospitality, tourism, and entertainment (HTE) industry. Current program activities emphasize tools and partnership practices (between the public and private sectors) to process information, produce actionable intelligence, and guide decision making to prevent and reduce crime. The emergence of intelligence fusion centers in the United States, which apply advanced analytic and predictive tools and depend upon data from public and private sector sources, underscores the growing importance of evaluating private sector participation in the fusion process in order to enhance national preparedness. One critical issue that needs to be addressed is how to strengthen the internal capacity of law enforcement, public safety, and private entities to embrace a collaborative process to improve information sharing and, ultimately, increase the ability to detect, prevent, and solve crimes.

Information gathered by state and local law enforcement agencies and other entities can be useful in fighting terrorism only if it is properly analyzed and correlated with other information to spur further investigation or contribute to a fuller intelligence picture. Criminal and terrorism-related intelligence is derived by collecting, blending, analyzing, and evaluating relevant information on a continual basis from a broad array of sources — including local, state, tribal, and Federal law enforcement authorities, other government agencies (e.g., transportation, healthcare), the general public, and the private sector.

Effective prevention efforts thus depend on the ability of all levels and sectors of government, as well as private industry, to collect, analyze, disseminate, and use homeland security and crime-related information and intelligence. At the state level, intelligence fusion centers — central locations at which local, state, and Federal officials work in close proximity to receive, integrate, and analyze information and intelligence — provide an opportunity to break down intelligence silos and transcend traditional bureaucratic turf wars. Unfortunately, gaps persist in the operation and management of information sharing-channels between law enforcement and the private sector. It is widely recognized that the added value of fusion centers "is that by integrating various streams of information and intelligence, including that flowing from the Federal government, state, local, and tribal governments, as well as the private sector, a more accurate picture of risks to people, economic infrastructure, and communities can be developed and translated into protective action."[1] However, despite the importance of joint preparedness efforts, evidence suggests that although most fusion centers describe an interest in expanding their relationship with the private sector, these partnerships were quite limited. In fact, "[i]nformation sharing with the private sector was often ad hoc and inconsistent."[2] Moreover, preliminary assessments indicate that fusion centers did not appear to be systematically importing and incorporating private sector data into their information/intelligence fusion efforts.

A review of Federal, state, and local

(Continued on Page 8)

[1] Masse, Todd, Siobhan O'Neill and John Rollins, Congressional Research Service. Fusion Centers: Issues and Options for Congress, #RL34070, Washington, D.C., July 6, 2007.
[2] Ibid.

Fusion Centers *(Cont. from 7)*

homeland security programs suggests that, as a Nation, we have made enormous financial and institutional investments in enhanced public safety programs that prepare our emergency responders for a range of threats and hazards, fortify government continuity of operations, and establish guideposts for high consequence sectors such as water, energy, chemical, and transportation. At the same time, there is little evidence that the government has dedicated resources to helping shape standards-based preparedness and protection programs in the CFS. This is particularly troubling given that 85 percent of the critical assets and key resources comprising our nation's 18 critical infrastructure sectors are privately owned and operated.[3] Moreover, not a single study has addressed the security-related requirements and training needs of the CFS or developed a systematic framework for assessing and building collaborative partnerships between law enforcement and the private sector for the purpose of detecting, deterring, preventing, responding to and recovering from terrorist attacks in the CFS.

The ISS, who brings subject matter expertise, project management experience, research skills, and outreach capabilities to the realms of homeland security, law enforcement, counter-terrorism, and emergency management, is actively engaged in efforts to address some of the current gaps in research and training, thereby improving collaboration and information-sharing between the CFS and the law enforcement intelligence fusion centers. Given its location, the ISS has focused on the hospitality, tourism, and entertainment industries within the CFS, which are widely recognized as vulnerable to terrorist attacks and frequently acknowledged as comprised of "soft targets." In addition, as the third largest retail sales industry in the Nation, travel and tourism have a major impact on the economy of the United States. The U.S. Department of Labor reports that one out of every seven people employed in the U.S. civilian labor force is directly or indirectly employed in the travel and tourism industry. According to the US Bureau of Economic Analysis, tourism related goods and services generated an estimated US$1.2 trillion in CY 2006.[4]

Critical steps in improving collaboration and information sharing between the CFS and fusion centers in Nevada include identifying the internal capacity of the CFS, engaging in partnerships with law enforcement, establishing community information networks, evaluating desired knowledge and skill sets, establishing appropriate and achievable training requirements, and defining mechanisms for sustainment training. This knowledge could enable law enforcement to more effectively design, operate, and manage information-sharing channels with the CFS.

To this end, the ISS has engaged in two recent projects that support the Southern Nevada Counter-Terrorism Center (SNCTC) and efforts to strengthen the information-sharing environment and enhanced community reporting of suspected terrorist activities. In 2008, the ISS authored and produced an educational DVD which provides a concise terrorism awareness message addressing the proper reporting procedures for counter-terrorism centers in Nevada. The ISS has distributed over 20,000 copies of the DVD around the world and to groups in Nevada that are believed to be the best sources of information (e.g. security professionals, public school security, airport security, cab drivers, and hotel public area personnel). Recently, the SNCTC selected the ISS to develop and implement a training project, the *Partnership Enhancement Research and Fusion* (PERFusion) program, to facilitate the exchange of information among the public safety community and their private sector security partners within Nevada. The PERFusion project seeks to fill a state and local priority requirement in information-sharing.

An important aspect of this training program involves designing an appropriate information technology platform that can effectively support and facilitate the exchange

(Continued on Page 32)

[3] US Department of Homeland Security, National Infrastructure Protection Plan, June 2006.
[4] U.S. Bureau of Economic Analysis (BEA), http://www.bea.gov/newsreleases/industry/tourism/tournewsrelease.htm (December 2007).

Self Storage Is Part of Today's Security-Threat Landscape

by Mark Wright

The national Self Storage Association is serving as a vital communication link between facility operators and homeland security officials.

You're making the rounds of your facility when suddenly you stop in front of a unit. You smell something, an unusual odor you can't quite put your finger on. It's just strong enough to get your attention, and only because you happened to be very close to the door as you walked past. "What the heck could that be?" you ask yourself.

You make a note of the unit number and continue on your way. Back in the office a few minutes later, you wonder if you should call someone, but you're worried about looking like an alarmist if it turns out to be nothing.

So, you run through the possibilities first — silently: Was it some kind of fuel? No, it didn't smell like that. Hmmm. You fish out the records for that unit to identify the tenant, but they're not much help: Just a guy who claimed to need some extra space while his home's garage was being remodeled.

The odor you smelled could turn out to be benign. Or, it could be evidence of a substance that might blow your facility sky high. What do you do? Who do you call? And how quickly should you react?

A New Era of Watchfulness

Bob Dylan's 1963 song, "The Times They Are A-Changin'," seems oh-so-relevant today — albeit in unexpected ways. To go to work and wonder whether you'll be an unwitting player in a dangerous plot targeting Americans, or discover a methamphetamine lab bubbling away in one of your units, is not the sort of job you likely contemplated when you got into the self storage business.

It's a new era, and like most new eras, the ability to adapt is paramount to survival. Adapting to today's threat-filled environment begins with acknowledging those threats. Yes, they're real. The unthinkable happens. Americans' innocence and denial collapsed along with the buildings that were struck and the lives that were lost on 9/11.

Is self storage on the must-have list of essential assets required by every terrorist sleeper cell or drug lord in the nation? Of course not. But for some it is. So, prudence demands watchfulness.

And watching is exactly what DHS — and the Self Storage Association, for that matter — is encouraging every SSA member to do. It's the first and simplest level of defense against potential threats.

"The big element in preparedness is educating the manager to spot suspicious behavior," notes SSA president and CEO Michael Scanlon. "We want to make sure we're doing everything we can as an industry to inform and educate our members so none of us becomes an unwitting enabler of terrorists or homegrown nuts."

Scanlon participates on SSA's behalf in a subgroup organized by DHS to update selected business and industry sectors on current security issues and threats, both manmade and natural. The subgroup in which SSA participates meets twice a year. A DHS spokesperson describes the process as a voluntary, two-way partnership that exists to be mutually beneficial for both the private sector and DHS.

SSA has posted important information obtained from its collaboration with DHS in the members-only section of selfstorage.org. (Access is restricted to members at DHS's request as a security precaution.)

Onsite Staff Key to Security

To avoid the "enabling" that Scanlon warns of, storage facility employees need to ask questions, notes Peter Beering, security expert, consultant, and speaker — and

(Continued on Page 10)

Self Storage Security *(Cont. from 9)*

author of the SSA publication, *Security for the Self Storage Industry*. Probably the most valuable security asset a facility can have, says Beering, is "the alert-employee who follows the program, asks questions and notifies people about things that don't look right. The entire system relies heavily on a well-trained counter person who says, 'This person is way too nervous. He or she is just behaving weird. I really need to let somebody know, even if it's just telling my boss.'"

"You have to build security in as part of the daily operation," counsels Beering. The recommendations outlined in the *Security for the Self Storage Industry* manual are intended to compliment existing facility management practices, he says. "The most effective security approach is to build it into the fabric of a company's culture."

Few know this reality better than people like Jordon Garrand, the Guardian Self Storage facility co-manager in New Windsor, New York, profiled in the October 2009 issue of the *SSA Globe*. Garrand's story shows how important it is to speak up when something about a tenant — or group of tenants — seems troubling.

"It showed the benefits of being observant, analyzing the activity, and being willing to communicate," observes New York Self Storage Association president Chris McGrath. McGrath had long ago developed a "Know Your Customer" booklet for NYSSA members emphasizing the importance of preparation and watchfulness. It details six simple steps, all to be initiated from the facility's counter, that guide the vetting of potential tenants. The SSA's Spotlight on Security program grew out of McGrath's work. (Click on "Self Storage Security" from the "Resources" menu at selfstorage.org for a free PDF copy.)

Technology Can Also Help

As central as the role of facility staff is in identifying problem tenants, no one is foolproof. Intuition by definition is inexact. That's why some storage operators have opted to give their security systems a high-tech boost, going beyond the basics of keypads and video cameras.

Christopher Barry, partner with Barrington, Illinois-based LifeStorage Centers, and Marvin Chaney, founder, developer, and owner of Ft. Lauderdale, Florida-based RoboVault, both chose threat detection systems from Norwalk, Connecticut-based Defentect (www.defentect.com).

The goal: Achieve early warning of terrorist efforts to build dirty bombs or other chemical, biological, radiological, nuclear, or explosive (CBRNE) threats. Barry and Chaney, respectively, wanted a solution that would integrate well with their existing computer-based security systems.

Without this technology, explains Barry, "we can only see what the eye can see. This gives us a level of detection that the customer wouldn't necessarily know we possess. We can find out if they're bringing in a volatile organic compound or other substances. You have to be more careful these days. We do a fairly thorough job of understanding what's going on at our properties."

Chaney is highly attuned to the post-9/11 security landscape, in part because of his facility's location — situated very near Port Everglades (where more than 5,300 ships call annually) and virtually across the street from the busy Fort Lauderdale-Hollywood International Airport. Chaney says he's "more concerned than I've ever been" about the possibility of someone transporting something harmful.

He thought his facility was tight as a drum, though. After all, it was built to withstand a category-5 hurricane, and the all-robotic storage system made theft of stored items unlikely. His fire suppression system was great, too.

Then he encountered a bucket of cold water in the form of an insurance rep who asked, "What are you doing about chemical storage? What if somebody stored material for a meth lab or nuclear device?"

That's when he "got lucky and ran across Defentect," Chaney says. "Insurance companies have a right to be concerned. What can we do to mitigate risk?"

(Continued on Page 25)

Facility Operators: How Intrusive Can You Be?

by Gary Camp

Whether it is a liquid oozing out of a unit, abnormal behavior that makes you suspicious, or even a strong odor coming from a unit, you must be careful not to jump to conclusions. Facility operators certainly must protect their properties, but in order to enter a unit, the situation typically must be classified as an emergency or maintenance issue.

It's All in Writing

"The facility owner's rights are derived from their lease agreement," said Scott Zucker, partner with Weissmann Zucker Euster, P.C., in Atlanta. Zucker acts as legal information counsel for the Self Storage Association.

"Within the lease agreement there is a provision typical to self storage rental agreements, a right-to-enter clause, which would set out [the owner's] right to enter for the purpose of maintenance, for the purpose of emergency, and other reasons that they could identify in the agreement," Zucker said. "Their rights are derived from a contractual agreement between themselves — the landlord and the tenant — to enter the space."

Some forward-thinking rental agreements include language that protects facility operators in regard to police searches and illegal activity. Well-written rental agreements might state that the facility retains the right to provide police with information concerning all of its tenants, and that the facility operator has the right to enter the unit where it is believed illegal activity is occurring inside.

"Typically, in a situation where they think there is illegal activity going on, or something suspicious or dangerous, that's when they call the police," said Zucker. "The police will investigate, and if they believe there is probable cause they'll get a search warrant and they'll go in the unit. We don't ever want to recommend to managers to enter into the unit to investigate something suspicious — that is for the police to do.

"There is no privacy violation by calling the police and saying there is some weird activity going on, coming-and-going in the middle of the night, strange deliveries," said Zucker.

The police will investigate and determine if there is cause for concern, and if necessary, they will execute the proper search warrants to be able to lawfully gain access to the unit in question. Proper documentation is necessary for anyone, other than the tenant that signed the rental agreement, to gain access.

"If they don't have the right paperwork, I don't care who they are, we can't give them any information or let them in," said Joe Stalloni, site manager with Sentinel Self Storage, located in Wilmington, Delaware. Sentinel Self Storage operates 11 properties in Delaware and Maryland.

"Now if they come in and they have all the proper paperwork, then we can do whatever they want to do. Personally, I would call our corporate manager, and discuss my concerns. I wouldn't personally call the police and say 'I think this guy is dealing drugs here.' I'd call the corporate office and let them handle it with the authorities."

Commonplace in rental agreement addendums are passages that clearly state what you can and cannot store. This also helps to avoid potential issues in the future.

The standard addendum on Sentinel Self Storage agreements includes verbiage that says:

You are agreeing not to store unusually valuable, sentimental, or irreplaceable items, such as heirlooms, jewelry, paintings, collectibles, or personal identification papers. In addition, items cannot be stored for health, safety, or security reasons: Perishable foods, explosives or flammable items, items that can give off noxious odors,

(Continued on Page 26)

Building and Fire Research at the National Institute of Standards and Technology

by Christopher J. Currens, MBA, MPA
Associate Director for Program Development, United States Department of Commerce
NIST/Building and Fire Research Laboratory

The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce and home to the Building and Fire Research Laboratory (BFRL). BFRL is the Nation's primary federal laboratory serving the construction and building industries, their materials and equipment suppliers, and the safety industries that help protect the public from the unwanted effects of fires, earthquakes, windstorms, and other natural and manmade hazards. BFRL operates within NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

BFRL strives to be the source for creating critical solution-enabling tools and promoting performance-based standards that are used by the U.S. building and fire safety industries to establish competitive leadership in domestic and international markets. In addition, BFRL has specific statutory responsibilities for fire prevention and control, earthquake hazards reduction, windstorm impact reduction, and building and fire safety investigations.

In many instances, BFRL conducts its research in partnership with the private sector. Thus, it is clear that BFRL is but one of a number of players involved in advancing the performance, productivity, and cost-effectiveness of built facilities. Increasingly, it is seen as a node in a larger network of organizations dedicated to better, more efficient, safer, and less costly facilities.

BFRL's five Strategic Goals — which are aligned with the critical national priorities identified by NIST — focus on:

1) Net-Zero Energy, High Performance Buildings

Buildings account for 40 percent of the United States' energy use and a similar percentage of carbon dioxide (CO_2) emissions, more than the transportation or industrial sectors. Emissions associated with buildings and appliances are projected to grow faster than those from any other sector. In order to ensure adequate supplies of energy and to curtail the projected growth of CO_2 emissions, it is essential that building energy consumption be significantly reduced. One way this can be achieved is through the introduction of innovative building technologies enabled by new measurement science.

In addition to energy issues, building operation practices face pressure to improve safety, security, and occupant comfort and health. Building control companies, equipment and system manufacturers, energy providers, utilities, and design engineers are under increasing pressure to improve performance and reduce

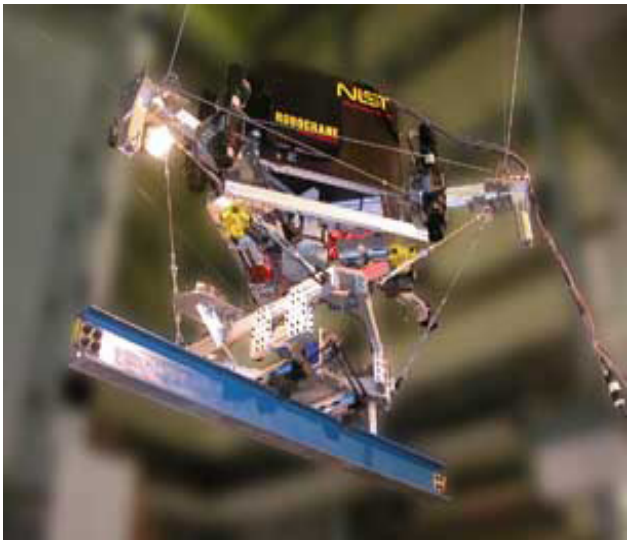
(Continued on Page 13)

Embedded Intelligence in Buildings

The NIST Virtual Cybernetic Testbed, a whole-building emulator used for a variety of integrated building system research activities.

Building & Fire Lab *(Cont. from 12)*

costs by developing cybernetic building systems that integrate more and more building services, including energy management, fire and security, transportation, fault detection and diagnostics, optimal control, the real time purchase of electricity, and the aggregation of building stock. Measurement science is lacking to enable these systems to communicate, interact, share information, make decisions, and perform in a "synergistic" and reliable manner. Specific needs include standard data models, communication protocols, user interface standards, security procedures, testing tools, and performance metrics. Overcoming these barriers is critical if cybernetic building systems are to be successful and if the U.S. is to obtain a significant share of the developing world wide market for such systems.



Automated and Integrated Infrastructure Construction Processes

BFRL researchers successfully equipped a unique cable-suspended six degree of freedom robotic crane — the RoboCrane™ — with real-time laser tracking and demonstrated an autonomous steel assembly process. This capability is one of many that BFRL is developing as part of the Intelligent and Automated Construction Job Site Testbed.

2) Advancing Physical Infrastructure Delivery

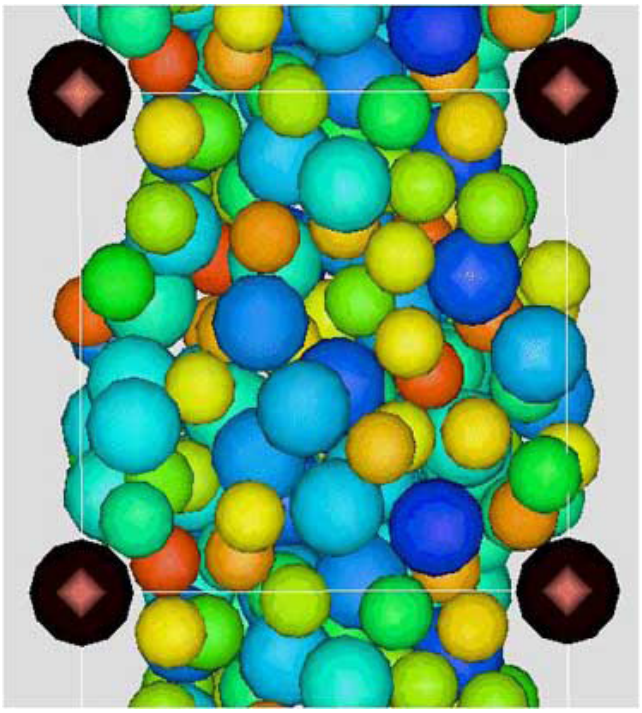
The nation and the construction industry face a projected $2 trillion cost-burden for renewal of critical infrastructure and increased global competition. During the past 40 years, construction productivity has declined at an average annual rate of - 0.6 percent. This trend is in stark contrast to all other non-farm industries (e.g., manufacturing) which have improved labor productivity at an average rate of 1.8 percent per year. Industry studies have identified inefficiencies ranging from 25 percent to 50 percent in current methods for coordinating labor and managing, moving, and installing construction materials. Other industries have realized their productivity advances largely due to the integration of information, communication, automation, and sensing technologies. Leading industry groups, such as the Construction Industry Institute (CII), Construction Users Roundtable (CURT), and FIATECH, have identified the critical need for fully integrating and automating construction processes. There is a lack of measurement science for determining construction productivity at both discrete and aggregate levels; enabling real-time monitoring and control of construction processes; enabling automated access to and integration of diverse information systems; and evaluating (and thus proving) the performance of promising automation and integration technologies in construction. Creating and validating the needed measurement science requires a neutral, representative, and accurately monitored environment in which the application of new construction technologies and processes can be evaluated.

3) Sustainable Infrastructure Materials

National and international economic growth cannot continue into the next century unless industries, especially high volume trades like the construction industry, dramatically reduce the amounts of natural resources and energy they consume and the wastes that they produce. To remain globally competitive while embracing sustainability, the U.S. construction industry needs to reexamine and redefine its practices: chemicals, materials, manufacturing methods, products, and waste disposal. Currently, construction materials, mainly concrete, steel, and polymeric materials, are being consumed at an annual rate of approximately $600 billion per year in new construction, and an additional $2 trillion in materials and construction products are required to renovate the existing

(Continued on Page 14)

Building & Fire Lab *(Cont. from 13)*



Service Life Prediction of Concrete Building and Infrastructure Materials

A computer model for predicting the flow properties of high performance concrete (HPC) aimed at designing HPC mixtures with optimum performance, both in the fresh and hardened states.

deteriorating U.S. infrastructure, according to the 2005 American Society of Civil Engineers Infrastructure Report Card.

Sustainability drivers include energy costs, global climate change, environmental regulations, disposal costs, resource scarcities, and population increases. Examples of environmental concerns include the need to reduce environmental impact through the inclusion of increased fractions of supplementary cementitious materials, like flyash (one of the residues generated in the combustion of coal) and slag (a byproduct of metal smelting), into concrete as well as reduce environmental, health, and safety concerns related to the potential release of nanoparticles from nanocomposite materials that are rapidly being introduced into the marketplace.

Sustainability decision software tools are currently being developed by industry, government agencies, and standards organizations. The efficacy of these decision tools, however, is greatly hampered by the lack of reliable sustainability input data, especially service life data for materials, components and systems, and the absence of measurement science for gauging this critical input. Without technically sound, thoroughly evaluated measurement science and data, the input available for making sustainability decisions is too crude and unreliable. This deficiency has been highlighted at a recent meeting hosted by the U.S. Department of Commerce to identify obstacles to enhancing U.S. competitiveness of internationally comparable metrics to measure the cost-effectiveness through sustainable manufacturing. At this meeting, industry expressed the "need for the establishment of internationally comparable metrics to measure the cost-effectiveness of sustainable manufacturing practices."

4) **Innovative Fire Protection**

The cost of fire in the United States is growing. In 2005, direct property loss due to fire was $10.7 billion and the total burden of fire on the U.S. economy is estimated to be around $270 billion/year. In 2005, the annual losses attributable to fire included 3,600 lives and 22,000 serious injuries. Fire service losses included about 100 lives and 80,000 injuries. Fires continue to

(Continued on Page 27)

Reduced Risk of Fire Spread in Wildland-Urban Interface Communities

BFRL conducts experiments of burning trees in order to validate predictions of heat fluxes and heat release from simulated trees using the Wildland-Urban Interface Fire Dynamics Simulator (WFDS). WFDS is a physics based numerical modeling approach which includes all modes of heat transfer (convection, conduction, and radiation).

National Center for Spectator Sports Safety and Security

by Walter Cooper, ED.D; Stacey A. Hall, PH.D; and Nick Nabors MBA/MS

The National Center for Spectator Sports Safety and Security (NCS4), established in 2006 at the University of Southern Mississippi, is the recognized leader in addressing potential threats and risks to the safety and security of sporting events.

Vision

To become a valuable national resource center that demonstrates development of security infrastructure systems and processes that will model solutions supporting multiple sports venue environments.

Mission

To conduct innovative research, provide internationally recognized academic programs, and develop integrated security solutions. The Center presently houses 12 staff members who work on a wide variety of externally funded projects. These projects range from a DHS Risk Management Training Grant, to a U.S. Department of Education Emergency Management for Higher Education Grant, and projects funded through both SEERI/ Oak Ridge, TN and The Mississippi Office of Homeland Security. Total funding is presently just over $8 million.

Continuous Improvement System

Those responsible for spectator sports security management at major sports events must plan, develop, and implement a highly effective all-hazards systems approach, capable of: training personnel, building effective communication channels, detecting, preventing, and responding to incidents, coordinating evacuation systems, monitoring game day operations, building a multi-discipline security team, and ensuring recovery and business continuity systems are in place. However, research indicates there are gaps related to effective risk assessment, training, and exercising capabilities at high consequence sports events (Cunningham 2007; Phillips 2006; Beckman 2006).

Acknowledging the industry's need to educate and train sport security professionals, and provide consistency in security management practices, the NCS4 developed a continuous improvement process for the effective security management of sport venues — the Sport Event Security Aware (SESA) system. The SESA system involves 4 key processes, including: 1) risk assessment, 2) training, 3) exercise, and 4) validation.

The DHS Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 is federal law designed to minimize or eliminate liability stemming from acts of terrorism. It was created after the 9/11 attacks in response to the multi-billion dollar lawsuits filed. The protection extends to companies' products or services that DHS has approved as being effective anti-terrorism. The NCS4 is in the process of applying for SAFETY Act approval for the SESA system. The ultimate goal is to implement the SESA system at all sport venues to ensure consistent safety and security practices.

Risk Management Training Workshops

The training program is designed to develop unique and essential expertise in sport venue security management. The goal of this training program is to create the standardization of sport event security risk management practices at collegiate sport events.

The Center consists of 18 individuals who are certified to administer this training at the Sport Event Risk Management Workshops (SERM). These trainers have backgrounds in the Campus Police, Athletics, Federal Bureau of Investigation (FBI), and Event Management and Emergency Management. DHS audited several of our workshops in 2009 and all of the trainers received high passing

(Continued on Page 28)

Security by Design: Creating Safe and Secure Commercial Facilities

New York architect and security expert Barbara A. Nadel, FAIA, describes how building owners, security consultants, and project design teams collaborate to enhance safety and security.

From high-rise office towers to retail complexes, commercial facilities serve a variety of public functions. The planning and design of commercial facilities requires the knowledge and skills of architects, who are licensed professionals responsible for public health, safety, and welfare. Together with the building owner, engineers, and other specialty consultants, architects are vital players on any building project team. The building owner, whether a private developer or public agency, determines the functions, operations, and construction cost of a project. An architectural firm, along with other consultants, is selected to develop the owner's vision into reality though the design process.

For many commercial buildings in major urban areas, high-rise towers and office buildings may be considered terrorist targets, especially those housing global functions or government agencies. In some regions, including South Florida, California, and Kansas, natural disasters, such as hurricanes, earthquakes, and tornadoes, are significant concerns to building owners and tenants. Floods, high winds, and seismic movement can damage and destroy buildings, making them uninhabitable. These local and regional site-related factors must be considered during the earliest planning stages of the design process.

Barbara A. Nadel, FAIA, founder of Barbara Nadel Architect, an internationally recognized architectural consulting firm, is an active member of the American Institute of Architects (AIA). Nadel's firm has consulted on numerous large-scale facility projects across the United States and overseas. She is a Fellow of the AIA. Nadel has served twice on the AIA board of directors, as New York Regional Director, and as 2001 AIA National vice president. She is editor-in-chief of the award-winning book, *Building Security: Handbook for Architectural Planning and Design* (McGraw-Hill, 2004). This preeminent handbook is an essential reference for security design, technology, building operations, and disaster planning. In May 2009, the AIA awarded Nadel the 2009 Edward C. Kemper Award for her significant leadership and service to the architectural profession, including her contributions to building security.

"After the events of September 11, 2001 there was a need for a comprehensive resource addressing building security in the U.S.," says Nadel. She assembled a team of national experts familiar with different building types, engineering, cost consulting, technology, and legal issues to share their knowledge. Her book, *Building Security*, discusses industry standards relating to design, construction, threats, and vulnerabilities. The events of September 11 have caused the design and construction industry to take a closer look at methods and techniques that enhance building safety and public security, says Nadel. Prior to September 11, the primary safety concern in most commercial high-rise buildings was getting people out of a burning building quickly and safely. After the 1995 Oklahoma City bombing of the Alfred P. Murrah Federal Building, and the collapse of the Twin Towers in New York City on September 11, architects, engineers, and owners now also consider the possibility of building collapse as a result of an explosion or bomb. Avoiding progressive collapse, through protective structural engineering design, is one of several security best practices that can be applied to construction of new commercial high-rise buildings that may be terrorist targets.

Ultimately, each site and building is unique, presenting many challenges to the design team. Architects must balance creativity and vision with client concerns, along with local building codes, and the budgets and schedules set forth by the owner. Large commercial projects may be subject to public design review by community boards, and other

(Continued on Page 17)

Security by Design *(Cont. from 16)*

stakeholders who may be impacted by new construction, renovations, or change of use to a commercial property. An example might include locating a hotel, which generates traffic at all hours, adjacent to a quiet residential neighborhood or school.

"Regarding building security, there is no one-size-fits-all solution," says Nadel. "Security is best addressed during the earliest planning stages when there is an opportunity to develop creative, cost effective solutions." Generally, public officials and building owners in New York City, Washington D.C. and other major cities are more concerned about terrorism than in other parts of the country because of the many potential targets in their midst. At the same time, every owner must balance the costs attached for implementing security, whether one-time costs for construction and technology equipment, or ongoing annual operational costs for security personnel or outside guard services.

Nadel described the security planning process, with a commercial high-rise building as an example. At the outset of the project, the owner commissions a security consultant to perform a threat and vulnerability risk assessment, which determines the potential threats to a building, site, and those who will occupy the building. The results of this report will determine the security measures to be implemented by the team, in response to real or perceived threats. During the design process, many tasks proceed simultaneously, especially under a fast-track schedule. Space programming occurs at the earliest stages, as the architect meets with the owner's team to determine the functions, spaces, number of personnel, hours of operation, and special requirements to be contained in a building. For example, a restaurant or cafeteria in an office tower may need a full kitchen and storage area, along with access to a loading dock. The architectural space program is a document that describes the number, sizes, and types of spaces required, along with a description of special requirements that might impact mechanical, electrical, plumbing, and structural engineering design. Architecturally, this would include the number of open and private offices, storage, public lobbies, conference rooms, and mechanical rooms for building equipment. Room sizes are expressed in square feet. Engineering concerns include areas to receive plumbing fixtures, special power and structural load requirements, and heating or cooling needs. After this data is developed, the architect can estimate the total square footage for the building, which is then used to develop a preliminary construction cost estimate. This estimate is then compared to the owner's budget. If the preliminary estimate is higher than the owner's budget, the project team generally reviews ways to cut back on costs, whether through reducing square footage, changing the materials, or building systems.

As the architect develops the conceptual schematic design in drawings and floor plans, the locations and numbers of circulation elements (stairs, elevators, entries, and exits) are refined, and checked against applicable building codes. Site planning is also underway, to determine vehicular and pedestrian circulation paths, and access routes for first responders, including fire trucks and ambulances. Security design is ideally integrated during the early design phases, when it is easier to make decisions and adjust for costs and operations. Design decisions might concern high performance window glazing to protect against heat gain, blast, or bullets, and exterior materials to harden the building against explosives or high winds, depending on the threat.

During the design development phase, the design elements are further refined. This can include determining lighting levels, fixture locations, interior finishes, furniture, room layouts, materials, and equipment. Sustainable materials, systems, and best practices will also be identified at this project stage. All materials, from flooring and walls to heating and cooling systems, will directly impact construction costs and the overall design.

The construction documents phase is when the design team completes the construction drawings and specifications that describe how the building will be constructed and the various materials and components that will be installed. Upon completion of the documents, the project goes out to bid and a

(Continued on Page 29)

Insurance, Meet Commercial Facilities: How Insurers Help Protect Commercial Facility Infrastructure

In order to preserve and protect their infrastructure, the owner of a commercial facility must be able to identify vulnerabilities and develop a plan to deal with them. This review and planning process requires a broad array of specific skills and knowledge, which the facility owner may or may not possess. There are a wide variety of resources to turn to for specific expertise, including governmental partners, consulting services, and trade or industry associations. One option is to use the services of their insurance company. This has the additional benefit of collaboration between two interested parties with closely aligned incentives. After all, both insurance companies and their policyholders/customers save money when there are fewer losses. Jennifer Naughton, a loss control services specialist with the Chubb Group of Insurance Companies, explains how this process works. Mrs. Naughton is educated in safety engineering and fire protection and worked in the insurance industry for 14 years.

The Policyholder Relationship

Policyholders come to Chubb with concerns about their safety procedures, their facility infrastructure, or their security practices. For example, a policyholder might be warehousing a supplier product that is flammable. The policyholder will then consult with Chubb about the risks this flammable product poses. Will their warehouses require new fire suppression systems, new storage protocols, or new safety training? Do the risks merit a redesign or product replacement/substitution? Or, should a policyholder incorporate a new chemical in their production process? Policyholders come to Chubb to discover ways to minimize the risk of accidents or lost work days. This may involve substituting chemicals in their production or finding new ways to dispose of waste. In the commercial facilities context, there are specific concerns about customer accidents, theft, fires, natural disasters, and other risks for damage or loss.

Policyholders possess industry expertise of their own, but as organizations flatten out and shed positions, individuals within a particular company will find themselves wearing multiple hats and thus have less time and attention to devote to niche issues, especially those requiring specific experience. Retaining a complete staff of security, safety, and infrastructure protection experts might be cost-prohibitive for some individual companies, especially smaller businesses. Insurance companies can afford to develop that kind of talent pool because they serve multiple companies. Loss control specialists will have backgrounds in fields like ergonomics, safety and health, civil engineering, fire engineering, and property management. Often they have years of experience within industry before moving to loss control, providing them with a grasp of the terminology and concerns of their policyholders. At its heart, loss control relates to risk management; therefore, understanding the basic concepts behind it is extremely valuable.

Policyholders tend to be enthusiastic about letting an outsider review their practices in this instance, because they know that the ultimate goal is to save them money, improve their bottom line, and reduce losses. In this strictly private interaction, there are few compliance issues and the insurer does not face the same coordination issues that public sector infrastructure protection programs have been known to experience. Here, the incentives are aligned for the two parties. What saves the insurer money from claims that do not have to be paid also saves the policyholder money from losses that do not harm the bottom line. The biggest sticking point is where changes require significant new investments. Policyholders may be reluctant to make large sacrifices for gains in the future. In other words, the loss control specialist has to be able to make a convincing case for the investments. The ideal recipients of this kind of review are identified by the policy underwriters, who actually manage the individual policies and set premiums. One incentive to offer policyholders who do undergo the changes that the loss control specialists recommend is that, should they reduce losses as

(Continued on Page 30)

Security and Infrastructure Protection at the Mall of America

A retail owner or operator faces a variety of tremendous challenges on a daily basis. Imagine, then, being the owner or operator of a retail facility which is also considered a national tourist attraction. A facility such as this introduces an entirely new array of concerns, threats, and vulnerabilities. The Mall of America, located in Bloomington, Minnesota, possesses the largest enclosed floor space of any retail center in the country, amounting to 4.2 million square feet. The Mall is comprised of 520 stores and, in 2006, hosted a total of 40 million visitors. The sheer scale of this facility, coupled with its unique nature as an American tourist attraction, make it a high-priority target. Dan Jasper, Director of Public Relations for Mall of America, took some time to explain how security and infrastructure protection work at the Mall.

The management challenges posed by the Mall's unique characteristics are difficult to overcome, but they also offer the Mall a chance to set the tone for security and safety practices that smaller facilities can emulate. The Mall's security director, Major Doug Reynolds, has presented to groups around the world and has testified before the House Homeland Security Committee on the Mall's security plan. The Mall of America was held up as an example of how to handle the issues of security, crowd control, disaster response, and the balance of safety versus accessibility.

In order to effectively secure a facility of such impressive magnitude, the Mall consists of a large security staff, over 100 officers. The Mall also boasts three canine units with dogs trained to detect explosive residue, items of high-end surveillance, and plain-clothes officers trained to mingle with shoppers undetected. Officers are trained in a wide variety of specialties; however, many officers are specifically trained on behavioral observation. The Mall is fortunate to have a large enough security staff that it conducts most of its training in-house, with staff members who are experts in various security skills often leading the training sessions. In addition, the Mall invests in ongoing training for its security staff as well as its regular employees. There is also cross-training between the Mall security staff and local law enforcement. Most importantly, the Mall interfaces closely with local law enforcement. There is even a substation of the Bloomington Police Department on site. Finally, while shoppers browse through stores, they can rest assured that there are always police officers at the Mall during operating hours.

Mr. Jasper said that most people are surprised to discover the depth of the security practices and the breadth of the security resources at the Mall. For example, deliveries are covered by a specific delivery protocol. All drivers and delivery personnel present identification and travel through security checkpoints. In addition, personnel must show identification at all times to prevent any infiltration into the Mall's non-common areas. Indeed, the entire security staff must pass a three-part interview process and a thorough background check before being hired.

The Mall's largest security concern relates to people bent on destructive behavior, be they lone individuals or concerted groups. This is not unlike other facilities which invite large numbers of people through their doors and serve both as functional facilities and meeting spaces for their customers. There have been many other malls and gathering areas where an individual has entered with a gun and opened fire, though the Mall of America has been spared such a tragedy. However, the Mall has developed a specific response plan for incidents such as this that involves the security department, the tenant stores, the police, and the staff. It is the sincere hope of everyone involved that this plan is never implemented. There are also emergency action plans for natural disasters; these plans are also rehearsed on a regular basis.

Obviously, security cannot be enforced without the cooperation of the millions of people who visit the Mall. Customers are encouraged to maintain vigilance of their surroundings at all times and keep their belongings and loved ones close at hand. Indeed, awareness

(Continued on Page 25)

Legal Insights

The SAFETY Act: Protecting Commercial Facilities in an Age of Terrorism

by Dillon M. Martinson, JD

Terrorists seek to inflict mass casualties, economic damage, and psychological shock. Consequently, commercial facilities — including shopping centers, office buildings, and sport stadiums — are potential targets for terrorists to attack. For example, in September 2009, FBI agents arrested Najibullah Zazi for plotting to bomb targets in New York. Although the exact targets are undisclosed, news reports claim that Zazi conducted internet searches on baseball and football stadiums.[1] On the same day as Zazi's arrest, the DHS and FBI released a joint bulletin warning that "analysis of detained operatives' statements, captured material, and domestic and overseas terrorist attacks indicates that [stadiums and arenas] are potential targets."[2]

Liability Concerns

Any business launching a new technology, product, or service has cause to worry about its exposure to liability. This is especially true for businesses developing anti-terrorism technologies for use in high profile commercial facilities. Two cases arising out of attacks on the World Trade Center illustrate the concerns high-profile commercial facilities face subsequent to a terrorist attack.

After 9/11, several injured victims and family members of victims who were killed in the terrorist attacks sued United and American Airlines, the Port Authority of New York and New Jersey, the World Trade Center Properties LLC, and the Boeing Company for failure to take adequate precautions in detecting and preventing terrorism.[3] The defendants moved to dismiss the claims by arguing that the terrorist attacks represented an unforeseeable criminal act that severed any liability, a defense that was successful in lawsuits arising from the 1995 Oklahoma City bombing.[4] However, the U.S. District Court for the Southern District of New York held that the plaintiffs could move forward with their claims, ruling that the defendants were warned of the threat of terrorism in New York and may be held liable because the attacks were within a class of reasonably foreseeable hazards.

In a 2008 decision, a New York appellate court upheld a jury's finding that the Port Authority of New York and New Jersey was liable for damages resulting from the 1993 World Trade Center bombing. The jury found the Port Authority to be 68% liable in the attack for its negligence in failing to provide adequate security and therefore liable to pay all of the non-economic damages resulting from the attack. This decision, combined with the 9/11 case, underscore the dramatic and costly reality of the liability concerns companies may face if their products and technologies are used in a terrorist attack.

The SAFETY Act Protections

One tool for overcoming these liability concerns is the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002

(Continued on Page 21)

[1] www.abcnews.go.com/Blotter/men-arrested-fbi-nyc-terror-plot/story?id=8618732&page=2.
[2] www.cnnac360.files.wordpress.com/2009/09/cip-fouo-notice-61-09-potential-threat-to-popular-sport-and-entertainment-venues3.pdf.
[3] In re September 11 Litigation, 280 F.Supp.2d 279, 287 (S.D.N.Y. 2003).
[4] The Homeland Security & Defense Business Council, Why Robust Use of the SAFETY Act is Critical to Homeland Security & How to Get There 5 (Oct. 2008).

Legal Insights *(Cont. from 20)*

(SAFETY Act),[5] enacted by Congress as part of the Homeland Security Act of 2002.[6] The SAFETY Act offers several levels of liability protection for providers of products and services that can be used to detect, identify, defend against, or respond to acts of terrorism. Typical anti-terror products and services include threat assessments, detection systems, blast mitigation materials, screening services, metal detectors, sensors, security services, and data mining software.

The purpose of the Act is to expand the creation, proliferation, and use of anti-terrorism technologies by creating a system of "risk management" and litigation management." The SAFETY Act allows firms that manufacture or provide a product or service that is a "qualified anti-terrorism technology" (QATT) to apply to DHS for protection from civil claims "arising out of, relating to, or resulting from an Act of Terrorism."[7] These protections are available only after DHS thoroughly reviews the product or service and approves the QATT for Designation or Certification.

The seller of a technology designated as a QATT receives the following protections:

1. Exclusive jurisdiction in Federal court for suits against the seller;
2. A complete bar on punitive damages and prejudgment interest;
3. Claims against the seller of a QATT are capped at the amount of liability insurance coverage required to be maintained by the seller (DHS sets the amount of liability insurance required for each QATT);
4. A prohibition on joint and several liability such that sellers can only be liable for the percentage of non-economic damages that is directly proportionate to their responsibility;
5. Any recovery by a plaintiff shall be reduced by the amount of collateral source compensation the plaintiff receives or is eligible to receive, including insurance benefits and government benefits.[8]

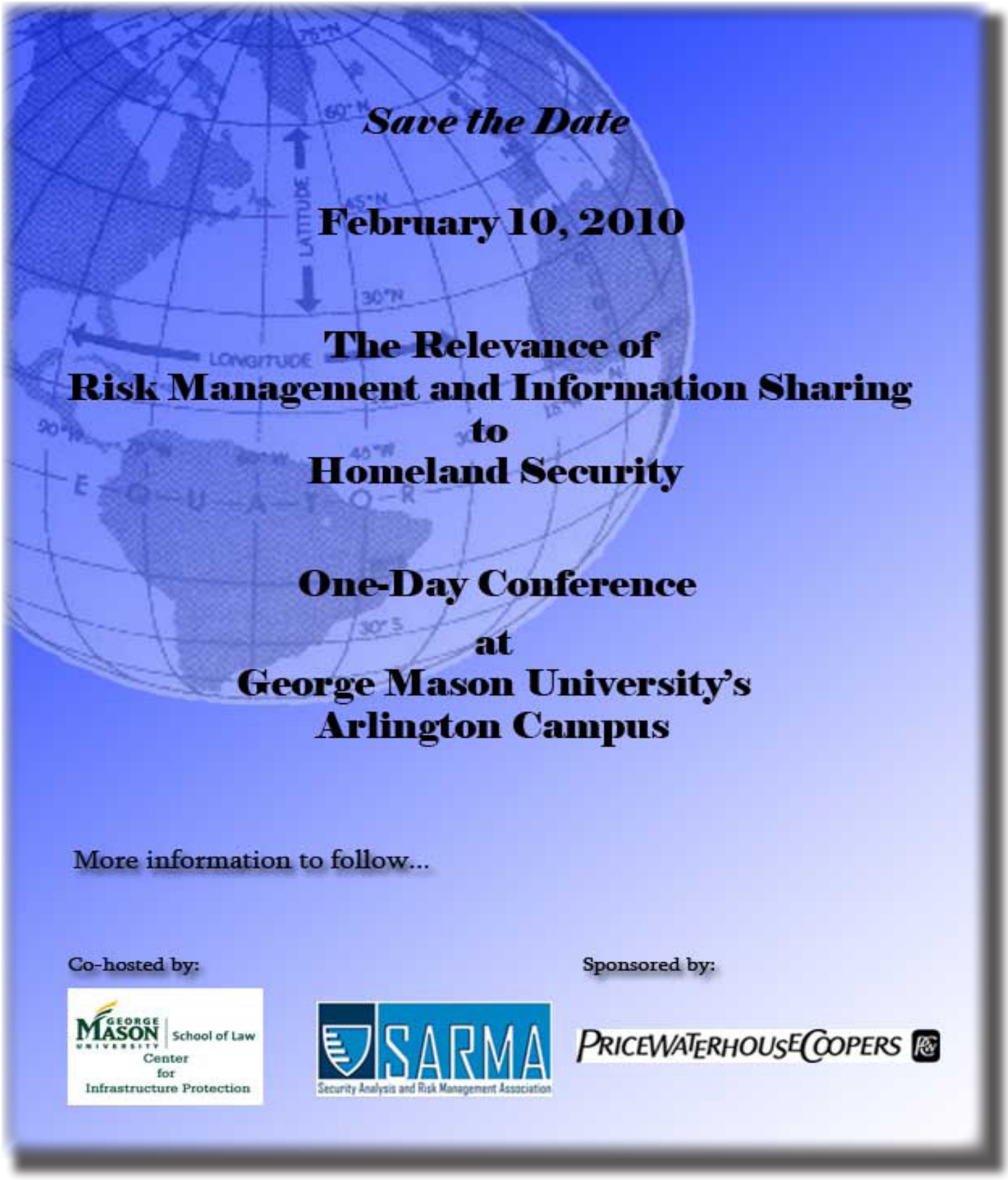
In addition to Designation as a QATT, a company may contemporaneously apply for Certification. Although Designation is a prerequisite for Certification, Certification is a separate application and requires a more vigorous review process. However, if certified, the seller of a QATT receives (1) a certificate of conformance; (2) placement on DHS's approved list for homeland security products; and most importantly; (3) a rebuttable presumption that the seller is entitled to the government contractor defense.

The government contractor defense is an affirmative defense that immunizes seller's liability for claims arising out of or related to an act of terrorism. Thus, Designation as a QATT caps seller's liability but Certification completely eliminates it. The statutory presumption of the government contractor defense can only be overcome by evidence demonstrating fraud or willful misconduct during the Certification process. Despite its name, the government contractor defense is available not only to government contractors but to all who sell QATTs to the private sector, federal government, or state and local governments.

Another significant protection of SAFETY Act Designation or Certification is that the only proper defendant in a civil suit is the seller of the approved QATT. In other words, all entities related to a technology other than the seller — including customers, suppliers, subcontractors, distributors — are immune from civil claims related to an act of terrorism using the technology. As customers of a DHS-approved technology, commercial facility owners and operators would have the right to seek immediate dismissal of a civil claim if sued following an act of terrorism that is proximately caused by the purchased QATT. This unique defense serves as a powerful incentive for commercial facility owners and operators to acquire and implement approved technologies as a safeguard for limiting liability as well as detecting, deterring, and

(Continued on Page 31)

[5] Support of Anti-terrorism by Fostering Effective Technologies Act, 6 U.S.C. § 861 (2002).
[6] Homeland Security Act, 6 U.S.C. § 101 (2002).
[7] www.safteyact.gov.
[8] 6 U.S.C. § 863(a)-(c).


Save the Date
February 10, 2010
The Relevance of
Risk Management and Information Sharing
to
Homeland Security
One-Day Conference
at
George Mason University's
Arlington Campus
More information to follow...
Co-hosted by:
GEORGE MASON UNIVERSITY School of Law
Center
for
Infrastructure Protection
SARMA
Security Analysis and Risk Management Association
Sponsored by:
PRICEWATERHOUSECOOPERS

Commercial Facilities *(Cont. from 2)*

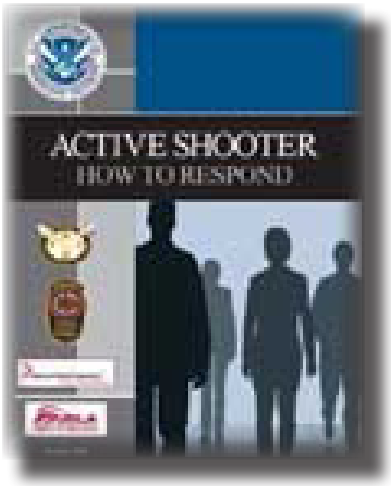
providing appropriate security tools, resources, and programs to individuals such as loss prevention and security directors at hotels, retail staff and shopping mall security directors, or stadium security managers, the Commercial Facilities SSA and its partners are empowering the sector and all of the members therein, and improving our national security posture in the process.

Recently Developed Protective Programs

Within the Commercial Facilities Sector, the Retail and Lodging Subsectors have worked closely with their public and private sector partners to provide the tools necessary to enhance sector preparation and resilience.

For example, the Commercial Facilities SSA and the Emergency Services SSA collaborated with law enforcement personnel and several private sector partners, including the National Retail Federation and the Retail Industry Leaders Association, to develop guidance materials concerning an active-shooter situation in response to several instances of shootings at retail venues.

The ***Active Shooter: How to Respond*** materials empower employees, managers, and human resources personnel to mitigate the risk of, and appropriately react to, an event involving an active shooter at the worksite. Products include a desk reference guide, a reference poster, and a pocketsize reference card. DHS developed these materials for a general audience and they are applicable to a variety of facility types in addition to retail establishments. The SSA has shared these documents with all of the 18 Critical Infrastructure and Key Resource Sectors.



DHS also worked closely with the Lodging Subsector to tailor an awareness tool to meet the specific needs of the U.S. Lodging Industry. The ***DHS Hotel and Lodging Advisory Poster*** provides the U.S. Lodging Industry with a tool to help hotel and lodging employees better understand a property's potential to be used for illicit purposes, spot suspicious behavior and items, and determine the actions they should take if they notice suspicious activity.

Developed by the DHS Office for Bombing Prevention and in close collaboration with the Commercial Facilities SSA and private sector partners, the ***Bomb-Making Materials Program*** serves as an outreach tool to local retail operators that sell household items commonly used in the making of homemade explosives (HMEs) and Improvised Explosive Devices (IEDs). It also serves as an outreach tool for local law enforcement to establish trusted private-public relationships with local retail operators. The program has led to the development of posters and register cards that give front-end store employees guidance on suspicious purchase recognition, as well as a ***Mall and Shopping Center Security Management Guide*** for use by mall and store managers in employee training. Additionally, DHS has developed a related training course for local law enforcement, focusing on the common materials used to construct HMEs and IEDs, and engaging retail stores in efforts to detect suspicious purchases.

With these tools, the grassroots of the Commercial Facilities Sector have been empowered with an opportunity to create a more secure and resilient place to work and play for every American. As Secretary Napolitano said, "when communities stand together and stand tall — so does our Nation."

It starts with people. ❖

For additional information on the resources mentioned in this article or other significant risk-reduction initiatives being undertaken in the Commercial Facilities Sector, please e-mail CFSTeam@dhs.gov or log on to www.DHS.gov/critical infrastructure.

Consumer Risks *(Cont. from 4)*

Nationally known stores or stores with a known physical presence were more attractive to some of the U.S. respondents who were more concerned with identity theft or fraud than their Israeli counterparts (Chi square = 112.6056, p =0.000). Functional risk is reduced to a very low level through the reliance on branded products, which remain the same in all retail locations. Additionally, among men and women, the younger the participant, the more likely he or she was to prefer to shop in person rather than online. The over-riding issues of perceiving shopping as a social event were more important for younger consumers.[6]

Women, in both the United States and in Israel, were more concerned about physical safety, but in the United States they appeared to be more willing to buy online than Israeli women. There may be a distinct difference due to some difficulties in using national credit cards versus international credit cards for the Israeli consumer. There are many online U.S. based retailers who only want to work with credit cards from a U.S. based bank to try to reduce financial fraud.

Practical Implications of our Study

Retailers should recognize that consumers are no longer care-free. They consider different risks pertaining to the possibility of physical harm when shopping during unsolved violent crimes in their neighborhoods or when threats of violence from unknown terrorists are reported in the media. During these times, retailers might want to promote use of their online stores. Some consumers, depending on their gender, are also concerned about financial risks — i.e., fraud and identity theft that might result from a purchase completed online. Retailers must reassure consumers that their passwords are protected and that their transactions are confidential through the use of encryption software.

Some consumers refuse to let fear of violence change their lifestyles and daily routines. They become hardy and tough-minded in order to avoid psychological risk. Shopping malls are natural meeting places that foster social interaction. Some consumers, especially younger ones, will continue to patron these facilities to interact with friends. Retailers might build more sitting areas where shoppers can relax or plug in their laptops while enjoying a cup of coffee. Finally, some consumer items — those that are bulky or very expensive — may not sell well online. They are associated with functional risk. Large items incur shipping costs while expensive items warrant careful hands-on inspection for quality. ❖

If you are interested in reading the original, full text article, please see: Carolyn E. Predmore, Janet Rovenpor, Alfred R. Manduley & Tara Radin, T (2007, October). "Shopping in an Age of Terrorism: Consumers Weight the Risks Associated with Online Versus In-Store Purchases." Competitiveness Review: An International Business Journal incorporating Journal of Global Competitiveness, 17(3): 170-180. http://www.emeraldinsight.com

[6] Choi, Jayoung and Loren V. Geistfeld. (2004). A cross-cultural investigation of consumer e-shopping. *Journal of Economic Psychology*, 25(6), 821-838.

Self Storage Security *(Cont. from 10)*

Are You Shaking Yet?

The more you wonder about this stuff, the easier it is to, well, freak out. That might be an understandable reaction, but it's not a helpful response. Over-reacting just shuts us down and/or makes us too suspicious.

As Beering notes, "Fear is nature's way of heightening our sensibilities to various risks. Most of us have a reasonable ability to assess risks. The thing to remember is, the vast majority of customers are at your facility for legitimate reasons. Often as not, standard operating procedures will ferret these things out. They're best practices, they're tried and true, and there's not a lot of magic to them. More than anything, it's just a matter of making sure people are actually following them."

Perhaps one of the best ways to dial down your anxiety level: Develop relationships with local law enforcement authorities — now, before you face a situation like the fictional sniff-test scenario we opened with.

As a DHS spokesperson who knows SSA well explains, facilities should "establish trusted partnership relationships on a local level. When all is said and done, the locals will be taking most of the action when something happens. Call them. Tell them who you are. Explain that you'd like to establish a relationship with them because of self storage's potential for — and actual role in — drug- and terrorism-related activities so you can share information quickly. And continue to nurture that relationship. When something happens, you want to already have established those relationships so that law enforcement can advise you quickly and respond appropriately."

During World War II, Uncle Sam used to warn that "loose lips sink ships." Today, however, America needs this industry's watchful eyes to be on the lookout for people who want to sink our nation's way of life and replace our freedom with fear. SSA will continue to make the latest information it receives through DHS available to members —whose keen senses serve as a vital part of America's day-to-day front line of defense. ❖

Mall of America *(Cont. from 19)*

and planning for a "worst-case scenario" does a lot to prevent serious harm. The Mall's security procedures work better when its customers are cautiously aware while they shop. For the most part, customers have been supportive of the security strategies; however, there has been contention over some policies. For example, a policy requiring everyone under the age of 16 to have an adult escort in the Mall on Friday and Saturday evenings was not only unpopular with the customers, but also with retailers, who were concerned that it would damage sales. Over time, the policy has proven effective and has been replicated in other malls around the country.

Similarly, the Mall requires the cooperation of its retailer tenants to act effectively. Currently, the Mall is working with them to update their emergency action plans. Should an incident occur, there is also a plan for locking down the Mall, similar to the lockdown a public school would implement. There are also protocols for the use of a variety of communication methods to quickly inform customers and retailers when a security threat is loose in the Mall. The entire staff has been trained in the Mall evacuation plan, so they can quickly move an exceptionally large number of guests to a safe area. Throughout November, the Mall will begin to prepare for the holiday season by holding practice sessions for the lock-down plan.

For the Mall of America,

(Continued on Page 28)

Facility Operators *(Cont. from 11)*

live animals, odors that can leak, spill or break out of their containers due to extreme temperatures, and any illegal or stolen property.

A well-written rental agreement can provide the necessary blueprint for avoiding litigation in the future. "We have the right to enter a unit at any time if we feel there is illegal activity," said David Dixon, vice president of development for Universal Management Company, an organization that manages 43 facilities around the U.S. "We also post in the office a notice allowing us to inspect any vehicle as it enters the property. Normally, we notify customers prior to any entering, but our rental agreement allows entry at any time. Obviously, we do not like to do this, but we can."

Maintenance and Emergencies

When a maintenance issue warrants immediate attention, it still makes sense to always bring along a witness, properly document and photograph the damage and building issue, and make sure that the reason for entering the unit is a valid one. The tenant should be contacted, if time permits, and asked to come let the facility manager in to the unit to repair the problem. But if the issue needs to be addressed immediately — such as a leaking roof or burst pipe — there isn't always time to wait for the tenant to arrive.

"If a tenant doesn't cooperate, and they have to proceed with the maintenance work, they will go in the unit and take a picture, have a witness with them, and proceed with the repairs that have to be done," said Zucker.

What about the situations that can be deemed "emergencies?" And we're not talking about the disgruntled girlfriend that wants access to her boyfriend's unit (the answer should be "no"). What about someone that truly needs access to a unit for a legitimate emergency reason?

Unless someone, or something, is in immediate danger, proper verification and a signature should be obtained before allowing anyone to enter a unit.

A typical clause in a rental agreement will include verbiage that clearly grants access in an emergency:

If there is an emergency where property, the environment or a human life is, in the opinion of the Owner, threatened, the Owner may enter the Space using all necessary force without the written consent of the Storer, but the Owner shall notify the Storer as soon as practicable. The Storer consents to such entry.

In most cases, it just requires written permission from the tenant to grant access to a third party. A notarized document is ideal, but a signed document or a fax can even work. Although a facility manager can easily say "yes," and grant access to a unit, it's best to always err on the side of caution, and avoid potential liability issues down the road. ❖

Building & Fire Lab *(Cont. from 14)*

kill more people per capita in the United States (by as much as a factor of two) than in most other developed nations. Fire losses from systemic causes are preventable.

Significant damage from wildland-urban interface (WUI) fires is on the rise in the United States and there have been two major WUI fire loss events in the last five years. The 2003 Cedar fire in California cost $2 billion in insured losses and destroyed 3,600 homes, while the October 2007 southern California fires displaced residents of over 300,000 homes. Overall, the trends suggest that the severity of the U.S. fire problem is growing.

There is an incomplete understanding of fire behavior, which hinders the development of innovative fire protection. Current prescriptive fire standards and codes stifle innovation in fire safety systems, technologies, and building design. To ensure fire safety in a cost-effective manner and to reduce fire losses, it is essential that adequate science-based tools are developed to enable the implementation of the next generation of standards, codes, and technologies that address the U.S. fire problem. Measurement science is lacking to reduce the risk of fire spread in buildings, to reduce fire spread in WUI communities, to ensure effective and safe use of emerging fire service technologies, and to derive lessons from fire investigations.

5) Disaster-Resilient Structures and Communities under Multi-Hazards

Natural and technological disasters cause an estimated $52 billion in average annual costs (and growing), with catastrophes like Hurricane Katrina and future "Kobe" earthquakes causing mega-losses exceeding $100 billion. Existing extreme load-related prescriptive requirements of building codes, standards, and practices stifle design and construction innovation and increase construction costs. The risk in large disaster-prone regions of the Nation is substantially greater now than ever before due to the combined effects of development and population growth. As noted by the National Science and Technology Council, "…a primary focus on response and recovery is an impractical and inefficient strategy for dealing with [natural disasters]. Instead, communities must break the cycle of destruction and recovery by enhancing disaster resilience."

The link between basic research and building codes, standards, and practices is weak. Further, the measurement science is lacking to: (1) predict structural performance to failure under extreme loading conditions; (2) predict disaster resilience at the community scale; (3) assess and evaluate the ability of existing structures to withstand extreme loads; (4) design new buildings and retrofit existing buildings using cost-effective, performance-based methods; and (5) derive lessons learned from disasters and failures involving structures. ❖

BFRL is constantly looking for opportunities to extend its impact through partnerships and collaborations. They encourage you to send them your thoughts and suggestions on how, working together, there may be even greater beneficial change and growth. You can visit their web site (http://www.bfrl.nist.gov/), and they look forward to hearing from you (bfrl@nist.gov).

Structural Performance Under Multi-Hazards

The US-90 Biloxi-Ocean Springs bridge (looking west toward Biloxi from the east shore). Simply supported superstructure spans were displaced and dropped north off their piers due to storm surge and wave actions during Hurricane Katrina in 2005.

Spectator Sports *(Cont. from 15)*

grades.

The SERM workshops are focused on building multi-agency collaboration capabilities among university command groups (CG). University command groups are composed of specialists from five distinct areas: campus police, athletic department, emergency management, fire/hazmat, and emergency medical/health services. University teams will learn to agree on basic concepts relative to: planning, risk assessment, training, exercising plans, and business continuity/recovery through scenario training modules. The expectation is for these university (leadership) teams to return to their respective universities and coordinate development of a sport event security management system. The Center successfully conducted 29 SERM workshops in 2009. These SERM workshops trained 1,061 individuals and 228 NCAA Division I, II, and III affiliated institutions. The evaluations of the SERM workshops by the participants have been very positive and uplifting. The participants express the need for the training because of the lack of training available for sport safety and security personnel. Participants also report that the trainers are of great expertise and present the curriculum efficiently.

The 2010 SERM workshops will start in April and will run through July. Currently, there are 37 workshops scheduled on the calendar with an invite list consisting of over 500 NCAA Division I, II, and III institutions. The workshop schedule and invitee list can be seen online at www.ncs4.com/workshop.

Future Developments

The Center staff is looking forward to moving into a new state-of-the-art facility early next spring. Plans include development of a demonstration EOC to be utilized for testing innovative products and for training purposes. NCS4 is also receiving numerous requests to provide training and other services to NAIA Member Institutions and Community Colleges, and to customize training for interscholastic sports venues. Undoubtedly, there are many challenges still ahead in the arena of protecting assets related to sports events. The NCS4 and its staff are well positioned to provide the resources needed to meet these future challenges! ❖

Mall of America *(Cont. from 25)*

security is a justifiable investment for resources such as the equipment, resources, training, and staff that they have devoted to solving security challenges. The high level of importance attributed to security is never more apparent than during the holiday season, when most retail stores experience their busiest shopping traffic. At the Mall, foot traffic increases dramatically during the holiday shopping season, with 40% of the year's visitors bursting through the doors. Incidents of minor theft increase and the amount of people situated in one place during the cold winter months raises concerns about health problems such as the transmission of seasonal illnesses. The Mall will respond to several emergencies a day during the season and dozens, if not hundreds, of customers will experience theft of their belongings, often because they lose track of them in the excitement of shopping. So this holiday season, if you shop at the mall, remember the dedicated staff and the hard work that goes into keeping you safe while you are there. It is one of those small holiday miracles that keep the season going. ❖

Security by Design *(Cont. from 17)*

contractor is selected.

Transparent Security

Nadel advocates the use of "transparent security," which is not visible to the public eye. "Security need not be obtrusive, obvious, or restrictive in order to be effective. A comprehensive security plan consists of three basic components: design, technology, and operations," she says.

The most cost effective way to plan for security technology is to include it in the overall design, and to select the appropriate equipment, rather than apply it after construction completion. Early planning can accommodate power loads, equipment locations, and ancillary support spaces, such as control rooms for closed circuit television (CCTV), and building monitoring systems. Architects must have a thorough understanding of how the building will operate, in order to adequately plan for security. The owner's operational policies and procedures for how the facility will be managed and function play an important role in this process.

Finding the balance between security and openness remains a major challenge in a democratic society, Nadel observes. Architects and designers must be willing to explore creative design solutions that still meet stringent security requirements. Building setbacks from the street, which mitigate the impact of vehicle borne improvised explosives (VBIEDs) can create opportunities for lively urban plazas with public art, fountains, level changes with berms, and low maintenance landscaping. Effective use of bollards, the elements designed to stop vehicles from ramming into buildings, with site design and landscaping, can make them less obvious in urban settings. These integrated design solutions are a vast improvement from the unsightly concrete Jersey barriers which appeared in front of many public buildings after September 11.

Site and landscaping elements, such as building setbacks, are a response to a specific threat of vehicle bombs, and will not address threats of chemical-biological-radiological-nuclear (CBRN) toxic materials within or outside a building, theft, petty crime, or workplace violence. Each threat requires a mitigating response, whether from design, technology, operations, or a combination of all three. Crime Prevention Through Environmental Design (CPTED) is a widely accepted technique that is frequently used in residential and commercial districts to enhance surveillance by community members. It relies on observation and awareness by residents and business owners to what happens in their neighborhoods, working in tandem with local law enforcement. Eyes on the street, low trimmed shrubs, and the maintenance of neighborhood properties are among the strategies used to maximize visibility and create safe, vibrant communities.

Building owners are on the front lines of providing public security, says Nadel, because they are responsible for the lives of thousands of people who live, work in, and visit their properties. Local law enforcement or insurers may require owners to maintain a certain high level of security based on tenants, location, or other significant factors. Occasionally, owners may provide high security levels to their commercial office properties as a marketing tool, to attract government agencies or contractors engaged in work requiring security clearance and confidentiality.

Nadel's advice to owners of commercial properties is to be aware of the potential security risks and liabilities if they choose not to provide appropriate security measures. A skilled architectural design and security team will collaborate with the building owner to effectively integrate design, technology, and operations. A commercial building should be open and inviting to the public, without making security obvious. "There are many opportunities to design buildings that are safe, secure, and represent design excellence. That is the goal of security by design," Nadel concludes. ❖

Commercial Insurance *(Cont. from 18)*

expected, this will be accounted for in the policy premiums. Premiums are determined by a complicated formula and the rate of losses and claims is one variable in that formula, but it does have an effect. A more direct effect is how high the underwriters will set the deductible.

Some clients will prefer to take on the additional risk that may occur as a result of avoiding some of the recommended changes, and that is reflected in their performance benchmarks. However, rarely does a company undergo the loss control process and not see some benefits. Clients are often as concerned about their regulatory compliance burden as with their losses and a loss control review will help with both. Simply having a fresh set of eyes reviewing their practices will mean the policyholder finds new solutions to their problems. Loss control specialists can also call upon a broad range of experience in industry dealing with similar issues, giving perspective to clients who are intimately involved in their own line of work. Loss control is as much about educating clients as it is about analyzing them.

Risk Management & Commercial Facilities

Within the commercial facilities sector, Chubb works with retail stores, museums, commercial real estate management companies who own facilities such as office parks and restaurants. The process is largely the same from sector to sector or industry to industry. The real difference is in the kinds of risks they face. The retail subsector in particular is extremely concerned about third party liability. The first step is to find out about the commercial facility's history, its previous risks, the plans for future use, the company's strategy, and every other piece of information that can help the process. Because the two parties' incentives are so closely aligned, there has not been a problem of securing effective information sharing. Policyholders willingly share everything they can in order to find the best improvement to the bottom line. In any event, most of the information a loss control services specialist would want has already been disclosed to the underwriters when the policyholder was originally insured.

Risk management is an ongoing process, not just for the clients, but also for the insurance company. It takes a great deal of continuing education and effort to stay current with new issues, threats, and solutions. The ultimate goal is to embed safety as a consideration in every step of the client's business process. In hard economic times, this is difficult. Clients want to preserve their bottom line by cutting costs and fewer people are doing more work as the organization flattens. This is when insurance companies may implement measures like online training to provide a lower-cost alternative while still stressing safety and accident prevention. The risk stays the same even if the resources to deal with it dry up. This need for specialized expertise will always be there, even as technologies and business conditions change and even as the economy rises and falls. So what message does this loss control services specialist want to convey? Mrs. Naughton noted that she felt the general public was largely unaware of her line of work. This niche profession tends to be largely a secret of insurance professionals and industry safety, security, and infrastructure protection experts. Advertising is not directed at the general public and not a lot of information is available to find out more about loss control or its role in making businesses safer and more secure. She said that she would like more people to know that she and her colleagues across the industry are working hard to prevent bad things from happening and that they have their customer's best interests at heart. The back and forth between insurance company and client is difficult enough without adding more conflict to the mix. At the end of the day, protecting people and property and reducing risk of harm is in everyone's best interest. ❖

Legal Insights *(Cont. from 21)*

preventing acts of terrorism.

Commercial Facilities and the SAFETY Act

Although the SAFETY Act protections can apply to all technologies, not just those used in commercial facilities, it is remarkable how few companies in the commercial facility sector have applied for coverage. The benefits from the SAFETY Act are tangible, the consequences for insufficient liability protections severe, and commercial facilities are known terrorist targets. Yet despite all this, the SAFETY Act remains relatively undiscovered.

In the first sixteen months of the SAFETY Act program, from October 2003 to February 2005, only six technologies were designated as QATTs.[9] From March 2005 to June 2006, an additional 68 technologies received SAFETY Act protections.[10] After DHS released a final rule clarifying and improving the SAFETY Act in 2006, there was a significant increase in the number of technologies receiving SAFETY Act protections. On July 30, 2009, DHS conferred protections on its 300th technology.[11]

While progress is being made, celebrating 300 designated or certified technologies may be premature. There are an estimated 1,800 stadiums and arenas in the United States, excluding high school stadiums and other small venues.[12] There are approximately 47,835 shopping malls[13] and an estimated 705,000 office buildings in the United States.[14] Given the number of technologies, products, services, software, security personnel, and emergency planning at each of these facilities, it is surprising that so few have applied for SAFETY Act protections.

One notable exception is the National Football League's "Best Practices for Stadium Security." This DHS-certified technology is a set of guidelines for stadium security management, including standards for game day operations, non-game day operations, threat assessments, and emergency planning. Similarly, DHS is currently advertising the January 2010 NASCAR Summit which is a three-day summit designed in part to improve security at NASCAR events.

Recent terror plots in the United States highlight the ever-present need to protect commercial facilities while legal precedent warns against insufficient liability protection. Notwithstanding these concerns, few companies have availed themselves of the unique protections offered under the SAFETY Act. Hopefully, as more high profile commercial facilities like the NFL and NASCAR take advantage of SAFETY Act protections, additional commercial facilities will follow suit and seek out qualified anti-terrorist technologies. Realizing the full potential of the SAFETY Act is in the best interests of commercial facility owners and operators, producers of anti-terrorism technologies, and the nation as a whole. ❖

[9] 6 C.F.R. pt. 25 (2006).
[10] Ibid.
[11] www.safteyact.gov.
[12] www.worldstadiums.com.
[13] www.census.gov/Press-Release/www/2005/cb05ff19-2.pdf.
[14] www.eia.doe.gov/emeu/consumptionbriefs/cbecs/pbawebsite/office/office_howlarge.htm.

Fusion Centers *(Cont. from 8)*

of information between the law enforcement community and private sector through on-line training and technical assistance. Based on SNCTC's priority task functions, ISS has designed and is implementing a trusted information exchange architecture that provides a single point of access to information resources (including electronically collected Suspicious Activity Reports), secure e-mail, mission-oriented bulletin boards and list services, a robust library of research information and documents, and supports a computer-based training (CBT) program of instruction for liaison officers. The PERFusion program involves the production of educational Specialty Skills Awareness DVDs, the design and development of web-based basic courses for Terrorism Liaison Officers (TLOs), and Fusion Liaison Officers (FLOs).

The educational Specialty Awareness DVDs are aimed to educate "frontline" populations in the CFS/HTE sector on suspicious terrorist activities and appropriate reporting procedures for the intelligence fusion centers in Nevada. Among these targeted groups of individuals are guest relations attendants, valets, bellmen, transportation operators, facilities engineering personnel, hotel registration desk staff, porters, food and beverage servers, hardware store managers, retail commercial property owners, and pharmacy owners. In short, these projects have been crafted with the goal of assisting the law enforcement community better identify and understand the obstacles or barriers to effective knowledge transfer and the successful methods for inculcating a counterterrorism preparedness culture within the CFS/HTE sector. ❖

**Robert J. Coullahan, CEM, CPP, CBCP is president of Readiness Resource Group, a veteran-owned small business in Las Vegas, Nevada. Dr. Nancy E. Brune is Director of Research at the ISS. Ross Bryant, PMP, is Director of Training at the ISS.*

Protecting Malls *(Cont. from 6)*

determine the conditions under which it makes sense to begin to implement the options considered in this analysis.

A reasonable approach may be to adopt a tiered implementation strategy. This would entail implementing any security options that are appropriate for today's environment and developing plans today for further measures to take if the environment changes for the worse. Those plans could address precontracting for equipment and services, collecting data needed to implement options efficiently, educating staff on the measures, and planning public relations efforts. Such efforts would reduce the time and disruption involved in implementing future measures. ❖

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1