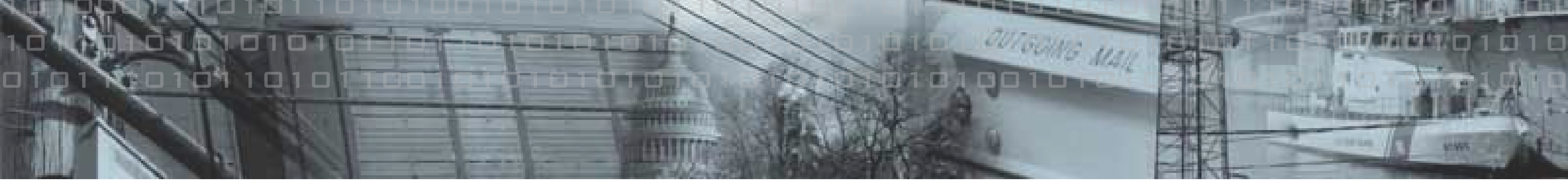


THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

FEBRUARY 2014

COMMERCIAL FACILITIES

EDITORIAL STAFF

EDITOR
Kendal Smith

PUBLISHER
Melanie Gutmann

JMU COORDINATORS
Ben Delp
Ken Newbold

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

VOLUME 12 NUMBER 8

With events such as the Super Bowl and the Winter Olympics claiming national and global attention, this month *The CIP Report* focuses on the **Commercial Facilities Sector**. Primarily industry owned and operated, this sector aims to ensure secure public access throughout the following eight subsectors: Public Assembly; Sports Leagues; Gaming; Lodging; Outdoor Events; Entertainment and Media; Real Estate; and Retail.

GEORGE MASON UNIVERSITY
School of Law
CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

First, Mark Camillo, CIP/HS Senior Fellow, explains why security must extend beyond an event itself to include transportation hubs, facility infrastructures, and vital resource feeds. Next, David R. Duda of Newcomb & Boyd Special Technologies Group examines the security risk assessment process for commercial facilities, including mitigation procedures for low, medium, and high risk facilities. Then, Michael Chipley of PMC Group LLC, Charlotte Franklin of the Arlington County Office of Emergency Management, and Roger Grant of the National Institute of Building Sciences introduce Integrated Rapid Visual Screening, a publically available tool enabling a quick and efficient risk assessment of a commercial building. Former U.S. Department of Homeland Security Deputy Secretary Michael P. Jackson then analyzes the role of technology in critical infrastructure security, particularly in sectors such as Commercial Facilities where information sharing is essential. Finally, Jeff Zisner, President & CEO of AEGIS Security & Investigations, describes several elements of a successful force multiplier program, used to detect pre-incident terrorist behavior.

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

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

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

Protecting Major Events: Security Measures Beyond the Venues

by Mark Camillo, CIP/HS Senior Fellow, George Mason University School of Law*

Rarely are the security concerns of large scale event security planners limited to what is 'inside the wire', namely the venue proper. The evolution of risk mitigation practices at major events in the United States since 1998 has significantly contributed to little or no disruptions of events of national significance. What began as a model for protecting the mega events in the homeland has morphed into a major event best practices guide that has shown success in the ability to either increase or decrease in scale, or serve as a 'menu of elements' from which a security planner might search in order to tailor an all-hazards security plan to a particular event.

The grand size and criticality of a Presidential Inauguration or the magnitude, duration, and iconic symbol of an Olympic games require an intense assessment of the risks posed and an engineered time-line that brings required resources to bear for the event. The National Special Security Event (NSSE) model has a solid track record of success since its inception in 1998. When it comes to implementing a layered security plan, it must be built on a platform of multiple organizations, each of which is a stakeholder in the successful outcome of the plan. As of January 2013 there have been approximately 40 NSSEs.[1] Some were large attendance events such as the 2002 Salt Lake Winter Olympics or small but high risk events like G8/20 Summits.

Credit, however cannot be solely taken by the respective venue operations. It is fair to say that the successful venue security operation is dependant in part on the entities that house and transport all those in attendance. In order to fill a stadium or arena with spectators, they will be arriving either from home or transportation hubs—i.e., train/light rail station, airport, or seaport. Large scale events often attract large capacity crowds. In large gathering spectator events such as golf or tennis, spectators often return multiple times, transiting via scheduled buses, trains, or shuttle vehicles. One successful practice adopted by event planners is establishing remote parking areas with dedicated transportation running on an advertised schedule.

When examining the manner in which crowds plan their attendance at a large scale event, hotels, transportation hubs, and transportation arteries should receive equal attention. A myopic approach to securing an event invites a crisis. As those who design the layered security plan for a venue, so should other security planners who focus on accommodations and transportation infrastructures. Understandably, resources are often strained when planning and implementing an all-hazards security operation at multiple venues. An Olympic or World Cup event can easily require a multitude of resources and personnel spanning in excess of 15 venues, all operating simultaneously.

The NSSE model dissects the overall Federal security responsibility into three parts: operational security, crisis response, and consequence management. The responsibilities fall under the purview of the U.S. Secret Service, Federal Bureau of Investigation, and the Federal Emergency Management Agency, respectively.

Can an event be disrupted from afar? The answer is yes. Can an event be impacted by malicious acts or even a natural disaster from afar? The answer is also yes. An example of event disruption from an external source in the United States can be found in the

(Continued on Page 3)

[1] Laurel J. Radow, "National Security Special Events: Transportation Checklist," *Domestic Preparedness*, January 23, 2013, accessed February 7, 2014, http://www.domesticpreparedness.com/Infrastructure/Transportation/National_Special_Security_Events%3a_Transportation_Checklists/.

(Continued from Page 2)

Anti-Terrorism

Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.

Counter-Terrorism

The practices, tactics, techniques, and strategies that governments, militaries, police departments, and corporations adopt in response to terrorist threats and/or acts, both real and imputed.

National Football League's 2011 season. Candlestick Park in San Francisco, CA experienced power outages during a night game due to an external power station problem. Although the outage was determined to be accidental, those with malicious intent witnessed a 'low tech/high yield' incident that caused disruptions at the game. The immediate nature of this type of disruption can bring a venue to a stand-still. Fortunately, emergency generators did their job until the normal power feed was restored.

In the case of the 2010 Vancouver Winter Olympics, planners were faced with the risks posed by the Sea-To-Sky Highway, a scenic but winding Oceanside road that connects Vancouver with Whistler, the site of the majority of alpine events. With transiting via ferry by sea or far inland the only other viable options, a plan was hatched to bifurcate the Olympic security operation into two stand-alone parts, thereby considerably mitigating the potential single point of failure posted by a possible Sea-To-Sky Highway closure. In the meantime, Canadian officials launched an aggressive plan to widen, straighten, and enhance the overall safety of the highway, anticipating unprecedented vehicle usage for the 16 day period. This collaborative effort between the provincial ministry of transportation and public safety entities typifies a successful horizontal integration plan.[2]

As the venue-specific security plans are being designed, so too should a plan be devised to provide the necessary coverage in between the venues, and at locations where event participants and spectators will likely converge prior to arriving at the venues. Best practices over the last decade or so has shown that anti-terrorism techniques, tactics, and procedures put in place at venues, coupled with counter-terrorism techniques, tactics, and procedures creates a very effective over-lapping capability. As an anti-terrorism plan provides robust prevention and protective elements at an official venue, a counter-terrorism plan properly implemented in areas and locations considered 'outside the wire' provides that critical spring-loaded capability to detect, deter, and disrupt attempts by those who wish to cause a disruption, but cannot penetrate the protective measures put in place at the official venues.

The Seattle-hosted World Trade Organization (WTO) meetings in 1999 illustrate how an event can be affected by a planned effort to impede the flow of participants/delegates. With the WTO meetings receiving a NSSE designation, the Federal lead agencies for operational security, crisis response, and consequence management quickly established partnerships with the state and local authorities to design, plan, and implement a layered security plan to address any potential acts of terrorism at the event site. Transportation infrastructure and hotel accommodations for delegates received attention through the public safety entities routinely tasked to maintain public order. What was discovered the first day of scheduled WTO events was a large organized group of protesters exercising their first amendment

(Continued on Page 4)

[2] Nasir Kurji and Ed Miska, "Vancouver 2010 Olympic and Paralympic Winter Games," (paper presented at the 2011 Annual Conference of the Transportation Association of Canada, Edmonton, Alberta), http://conf.tac-atc.ca/english/annualconference/tac2011/docs/t1/kurji.pdf.

(Continued from Page 3)

1999 WTO Seattle Protest*

rights on the streets in proximity to the official venue and in front of hotels where delegates were residing. This organized crowd succeeded in delaying and in some cases preventing delegates from accessing the event site. Simultaneously, small groups of individuals described as 'Anarchists' were observed vandalizing properties near the event site, and in some cases, causing destruction on the streets. The delays caused by the protest groups and acts of vandalism and destruction by 'Anarchists' ultimately led to the Governor of Washington deploying the Washington National Guard in order to assist law enforcement authorities in restoring order in the streets of Seattle. The WTO meetings eventually resumed, but the successful disruption of the event was clearly caused by actions beyond the official venue. As with all NSSEs, the After Action Report was studied by cities with scheduled upcoming events considered controversial, and measures were put in place to identify, deter, and disrupt any planned violent protests. The World Trade Organization 1999 Seattle Meetings witnessed the first NSSE that experienced civil disturbance.

As mega events are being planned and hosted internationally, incidents such as the bombings at a train station and on a bus in Russia in advance of the 2014 Sochi Winter Olympics are notable incidents where those with malicious intent will strike outside the official event site to bring attention to their cause.

Conclusion

We have gained considerable experience since the arrival of the 21st Century in regards to securing major events. Examples noted in this article are only a few of several that reinforce the importance of extending the venue security mind-set out to transportation hubs, facility infrastructures, and vital resource feeds that are critical entities in relation to a major event. Radicals, whether they are conspiring from abroad or self-radicalized at home, have learned that their pathway to least resistance on a nefarious act is finding soft targets. Event security planners do not always have the luxury of knowing exactly when and where bad things might happen, but do have the knowledge, skills, and abilities to expand anti-terrorism and counter-terrorism techniques and tactics beyond the venues to related infrastructures.

**Mark Camillo is internationally recognized as a law enforcement and security professional, with exceptional expertise in the area of emergency preparedness operations. He is credited with directing the security operations of some of the most critical infrastructures in the world, and served as the Olympic Coordinator for the 2002 Salt Lake Winter Olympics. Mark is currently the Senior Vice President for Strategic Planning at Contemporary Services Corporation, the United States leader in event security and crowd management.*

**Photo Courtesy of HistoryLink.org.*

Determining Appropriate Protection for Critical Commercial Infrastructure

by David R. Duda, Associate Partner, Newcomb & Boyd Special Technologies Group*

When one thinks of critical infrastructures, some come quickly to mind: the water system, the power grid, the Internet, dams, bridges, roads, air and rail transportation to name a few. Commercial buildings may not occur to the average individual as critical infrastructure, but they are considered as such by the Department of Homeland Security (DHS) and ASIS International. If we think about the impact of the 9/11 attack on the Twin Towers, we understand why. The attack on the Twin Towers cost nearly 2600 people their lives, and launched the United States into a long term war on terror that has increased the national debt approximately 1.5 trillion dollars.[1]

ASIS International's 2011 Critical Infrastructure Resource Guide[2] lists public assembly, sports leagues, gaming, lodging, outdoor events, entertainment and media, real estate (office buildings, mixed use facilities, apartments, etc.), and retail in the commercial facilities sector. Of course not all commercial buildings are "critical" infrastructure. The loss of a storage facility may have little impact on the owner and no impact on the economy or nation as a whole. This means we must evaluate the critical nature of our commercial infrastructure to determine what security or countermeasure we should implement to protect it. This is the purpose of a security risk assessment.

The Security Risk Assessment

Several well established risk assessment methodologies are available, but in essence, to determine a risk level, most rate the assets (people and property) or infrastructure in terms of its critical nature (impact of a loss); threats in terms of their severity and credibility; and vulnerabilities in terms of their exposure. We then concentrate our efforts on mitigating or reducing the higher risks by reducing or eliminating vulnerabilities. In most cases we cannot affect the critical nature of the assets, or the severity of the threats. We can only reduce vulnerabilities.

A typical security risk assessment will use the company's historical data and current intelligence to determine the design basis threats for the development of the risk matrix. These may include:

- Vandalism of property.
- Theft of property.
- Unarmed attack (use of fist or brute force of a nature insufficient to cause death).
- Armed attack.
- Propelled or thrown explosives (rocket propelled grenade, Molotov cocktail, etc.).
- Hand delivered explosives (package bombs or placed bombs) attacks.
- Vehicular delivered explosives (vehicle bomb) attacks.
- Chemical, biological, or radiological (CBR) attacks.
- Cyber-attacks.

Each of these design basis threats will be evaluated against each asset considering various factors to determine vulnerabilities to the threat. A commercial facility that houses a work force of 5,000 will generally require more security than one that houses 5 people. Exceptions can be found in government or military facilities (as the nuclear silo that houses 2 men and weapons that can extinguish the lives of hundreds of thousands, if not millions), but it is generally true in commercial facilities. Likewise, a company that is considered an

(Continued on Page 6)

[1] Kimberly Amadeo, "How the 9/11 Attacks Still Affect the Economy Today," *About.com*, October 22, 2013, http://useconomy.about.com/od/Financial-Crisis/f/911-Attacks-Economic-Impact.htm.

[2] Critical Infrastructure Working Group (CIWG), *Critical Infrastructure Resource Guide 2011*, (ASIS International, 2011), https://www.asisonline.org/ASIS-Store/Products/Pages/Critical-Infrastructure-Resource-Guide-2011.aspx?cart=5c010ddef61943ef8287634d665d443b.

(Continued from Page 5)

icon of the American way of life may make a more attractive target than one that is not a household name.

By examining various "what if" scenarios for each risk, countermeasures are theoretically applied, and the process repeated, to evaluate the proposed countermeasures. A comprehensive security program is then developed around the most effective countermeasures to include the appropriate physical security components, policies and procedures, and staffing and training.

Figure 1 - Arlen Specter Headquarters and EOC, Centers for Disease Control and Prevention, Atlanta, Georgia

Figure 2 - Cobb Energy Performing Arts Centre, Atlanta, Georgia

Risk Mitigation - The Security Program

A comprehensive security program that balances the use of protection resources (people, physical security systems, and policy and procedures) is generally the most effective. A weakness in any one of these components can negate the effectiveness of the other two. Perhaps the best illustration of this is that the best locks are useless if we don't remember to lock the doors.

Low Risk Security Facilities

Physical security for low risk commercial facilities may include a basic burglar alarm system, a few cameras, and the use of good lighting. Security policies and

(Continued on Page 7)

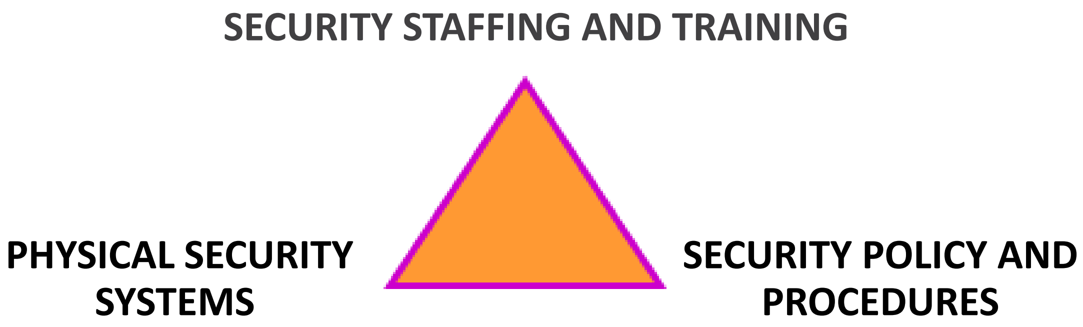

SECURITY STAFFING AND TRAINING
PHYSICAL SECURITY SYSTEMS
SECURITY POLICY AND PROCEDURES

Figure 3 - The Three Components of a Comprehensive Security Program

(Continued from Page 6)

procedures may include those that address disaster management and emergency response (evacuation or shelter-in-place), key control and accountability, opening and closing procedures, video management, pre-employment screening (background checks), prohibited items and substances, drug and alcohol use, and termination. There may be no dedicated security staff, or a few contracted security officers. Security functions may be performed by personnel with other duties. Training may include fire drills and safety and security awareness. The risk assessment will determine the extent to which facilities such as retail buildings, apartment complexes, condominiums, and self-storage facilities will fall into this category. Some of these may not fall into the realm of "critical" commercial infrastructure.

Medium Risk Commercial Facilities

Medium risk facilities may also have card reader controlled access, a computer based visitor management system, intercom systems and/or emergency call stations, and an expanded video surveillance system. Additional policies and procedures may be needed to address security responsibility and accountability, access control (who gets a badge, who gets access to what, who authorizes badges, etc.), workplace violence prevention and intervention (including bomb threats and active shooters), use of archived video, and security post orders, general orders, and special orders. Security staff may include contracted or proprietary security officers. Additional training may be needed for proprietary security staff. The risk assessment will determine the extent to which facilities such as office buildings, conference centers, mixed use facilities, hotels, and retail centers will fall into this category.

(Continued on Page 8)

Figure 4 - Navy Federal Credit Union, Pensacola, Florida

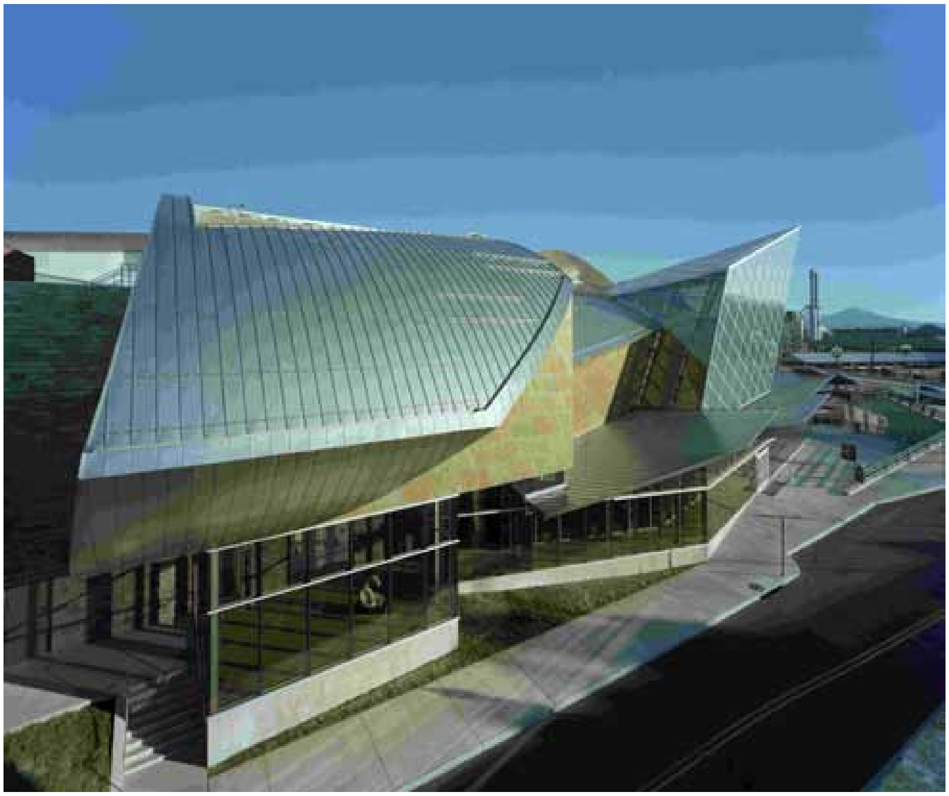


Figure 5 – Taubman Museum of Art, Roanoke, Virginia

The Trend to More Video

Much of the commercial sector is trending towards more video cameras and the use of higher resolution megapixel cameras. Two and five megapixel cameras have become very popular. It is not uncommon for a large commercial facility to have hundreds of video cameras covering vehicle entrances, parking lots, building entrances, emergency exits, loading docks, and infrastructure that is critical to the operations of that facility (such as data centers, server rooms, electrical switchgear, generators, and uninterruptible power supplies).

It is difficult, if not impossible, for an operator to watch a multitude of video camera displays and main-

(Continued on Page 9)

(Continued from Page 7)

High Risk Commercial Facilities

A high risk facility may also have vehicle stand-off enforced with crash-rated barriers (both fixed in place and operable), facility hardening for ram, blast, and ballistic resistance, and X-ray screening systems and magnetometers. Additional policies and procedures may be needed to address occupational safety and health; personal use of company assets; property control, marking, and disposal; and information handling (disclosure, marking, storage, disposal, and destruction). The risk assessment will determine the extent to which facilities such as stadiums, museums, convention centers, casinos, and central banks will fall into this category.

Figure 6 - Taubman Museum of Art, Roanoke, Virginia

(Continued from Page 8)

tain vigilance. Mental fatigue and boredom will set in and the operator will miss important events. This makes it imperative to automate the video surveillance system such that selected monitors only display video when triggered by potential alarm events. This can be done by connecting alarm outputs from the security management system to the video management system and configuring the system such that various events (such as door forced, door propped open, and emergency exit used) cause the video covering the event to be displayed on the alarm monitors. Built-in motion detection can also be used, but is limited to interior locations due to potential nuisance alarms.

Not all cameras cover areas where such alarm triggers exist. For example, a camera covering a fence line does not have any type of switch to act as a trigger. In this case there are special intelligent video analytics software and hardware systems that can provide detection of unwanted behavior, and alert the operator while initiating recording of the scene in question. Some of the behaviors that can be analyzed include:

1. Directional line crossing: virtual line crossing (tripwire) for human and vehicular movement.

2. Movement-in-zone: detection of human or vehicular movement in secure zones where no movement is expected, with filters for direction of movement.

3. Suspicious (abandoned) objects: detection of abandoned objects in an area of interest with filters for size and length of time object is present.

4. Loitering: detection of person sojourning within a defined zone for a user-defined period of time.

5. Tailgating: detection of person or vehicle crossing a line within a user defined time interval after another person or vehicle. This can be integrated with access control systems.

6. Crowd size detection: alarm generated upon crowd size reaching a user-defined threshold.

7. Moving water vessel: detection of water vessel movement, filtering out waves, sun reflections, and typical waterscape phenomena.

8. Illegally-parked (stopped) vehicles: detection of vehicles stopped in one or more no stopping zones beyond a configurable time threshold.

9. Object removal: detection of object removal from a customer-defined region in a video camera's field of view.

10. Asset protection: detection of the removal of up to 20 objects from a camera's field of view. The event is reported when an object is removed or hidden for more than the specified amount of time.

11. Two-man rule alerts: detection if less than 2 people are present at any time.

(Continued on Page 10)

Figure 7 - BlueCross BlueShield of Tennessee, Chattanooga, Tennessee

(Continued from Page 9)

12. Fallen person (slip and fall): detection within seconds of transition from a person's vertical position to horizontal/angled position.

It should be noted that no single video analytics system provides all of the above mentioned capabilities. Additionally, they are more often than not licensed on a "per behavior-per camera" basis and can be expensive to deploy on a wide scale. Therefore they are implemented for specific cameras (such as the camera covering the perimeter fence) and for specific behaviors (such as directional line crossing or trip wire). It is anticipated that the use of these analytics will continue to grow as more become aware of their capabilities and as costs decrease.

Conclusion

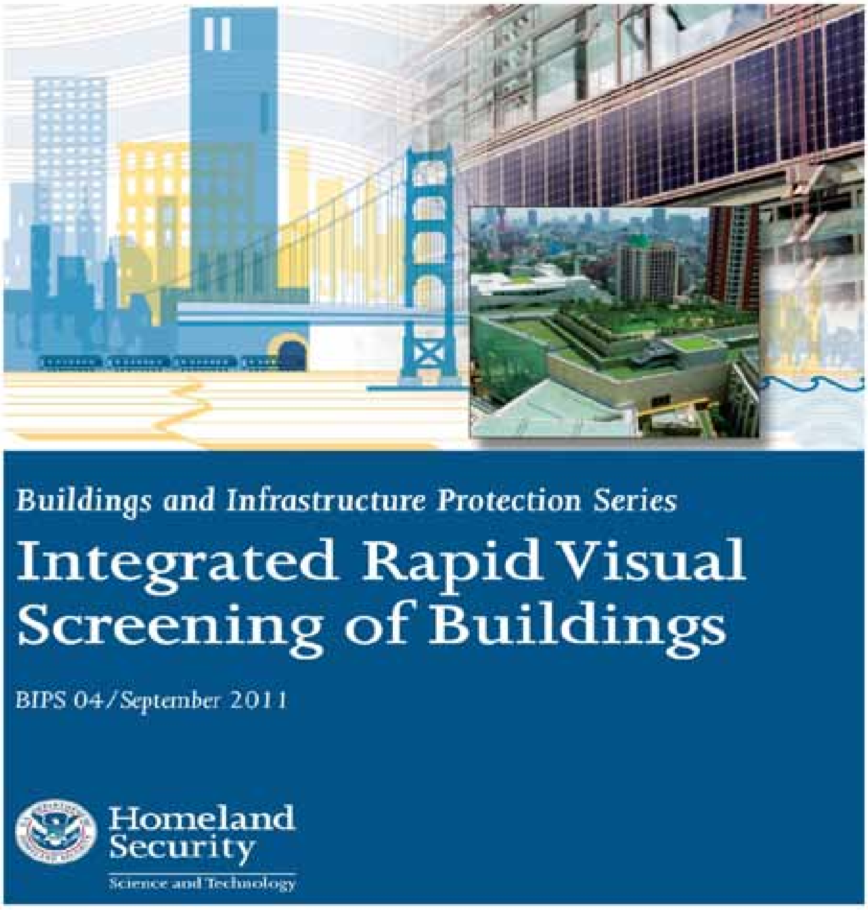
Many commercial facilities are considered an important part of the national critical infrastructure. Additionally, these facilities have infrastructure that are critical to the mission of the facility. Just how critical and to what level each should be protected is determined by a security risk assessment. Once the risks are evaluated, various countermeasures or mitigation means are applied and the risk re-evaluated. This process is repeated until effective mitigation measures are determined. Commercial facility owners and operators can find assistance through professional security consultants, the Department of Homeland Security, and ASIS International. The International Association of Professional Security Consultants members provide independent objective security advice on a range of specialties. DHS offers assistance to private sectors through many avenues; one is the DHS Private Sector Resources Catalog. A similar resource offered by ASIS International is the Critical Infrastructure Resource Guide, published by ASIS International's Critical Infrastructure Working Group.❖

**Mr. Duda is an associate partner with Newcomb & Boyd Special Technologies Group (http://security.newcomb-boyd.com). In his 29 years with the firm, he has provided security consulting and engineering services for their various clients, including Fortune 500 companies, colleges and universities, hospital systems, U.S. Government agencies, United States Armed Forces, and state and local municipalities. He served in ASIS International's Critical Infrastructure Working Group in 2012 and 2013.*

The Infrastructure Security Partnership
2014
Critical Infrastructure Symposium
Disasters are Personal. Resilience is Regional. Partnerships are Strategic.
www.tisp.org

Using the Integrated Rapid Visual Screening Tool to Conduct Physical Security Site Market Surveys of Commercial and Federal Facilities

by Michael Chipley, PMC Group LLC,
Charlotte Franklin, Arlington County Office of Emergency Management, and
Roger Grant, National Institute of Building Sciences*



Buildings and Infrastructure Protection Series

Integrated Rapid Visual Screening of Buildings

BIPS 04/September 2011

Homeland Security

Science and Technology

About IRVS

Integrated Rapid Visual Screening (IRVS) is a quick and simple tool developed by the DHS Science and Technology (S&T) Directorate's Resilient Systems Division (RSD) that determines the preliminary risks, resilience, and multi-hazard interactions of a facility: commercial or federal. The IRVS methodology can effectively and powerfully compute the level of risk to different facility types from a broad range of natural and man-made hazards. DHS S&T RSD has developed IRVS in modules for Mass Transit Stations, Tunnels, and Buildings. This article will focus on the Buildings version.

The IRVS Basic for Buildings has been made available to the general public free of charge and provides:

- Numeric risk and resilience scores that produce a quantification of relative risks, and an understanding of the most dominant features of the building controlling overall risk.
- An understanding of resilience, potential down time, and economic and social implications if a building is affected by a catastrophic event.
- Ranking of vulnerabilities and consequences within a community, indicating which buildings are more at risk and require higher protection.
- Identification, collection, and storage of vulnerability data that can then be re-examined both before and after protective measures are put in place.

Results obtained from the IRVS Basic for Buildings can be used for a range of important applications, including:

- Prioritizing facilities for further evaluation.
- Prioritizing mitigation needs.
- Supporting higher-level assessments and mitigation options by experts.
- Allowing for efficient resource allocation.

(Continued on Page 12)

(Continued from Page 11)

- Developing emergency preparedness plans in the event of a high-threat alert.
- Planning postevent evacuations, rescues, recoveries, and safety evaluation efforts.
- Evaluating suitability to meet owner's needs and objectives for facility use.

IRVS Basic for Buildings is built on an MS Access database platform, with several enhanced security, administrative, and operational procedures to ensure assessment data is properly protected. A key IRVS feature is the User Manual, which has examples of building features and elements for every question and contains the embedded knowledge of multiple subject matter experts garnered over the past several years. All of the IRVS modules have been tested and validated with multiple public and private users across the country.[1]

In 2012, DHS S&T RSD released a new IRVS module based on the IRVS Basic for Buildings which automates the process of conducting an Interagency Security Committee (ISC) evaluation of federally owned or leased facilities. The IRVS plus ISC is a state-of-the-art resource enabling federal and local government, engineers, architects, security specialists, property owners, and developers to conduct a risk assessment and complete the Pre-Lease Physical Security Plan that must be submitted by the offeror of lease space intended for federal government employees.

This tool, using a very detailed question checklist, combined with visual criteria, allows a team of one to two assessors to complete a risk and resiliency assessment in a fraction of the time (2 to 4 hours) needed to complete the traditional assessment process. This newest IRVS release follows the process and requirements established in the August 2013 *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard.* The IRVS plus ISC follows the same tabular and checklist format of the IRVS Basic while also following the ISC Risk Management flow chart. After establishing the target facility security and baseline protection levels, the assessor can develop a strategy to address identified vulnerabilities—either through mitigation measures (Capital Project; Work Order; Plans, Policies and Procedures; Personnel; or Other), or by providing a rationale for risk acceptance (historic property, site conditions, short-term occupancy, funding, etc.). The IRVS plus ISC also has extensive reporting, analytical, and exporting capability. Similar to the IRVS Basic for Buildings, it includes an All Details report with an Executive Summary; all 86 ISC questions, answers, and comments; pictures; and a summary of additional documents used for the assessment (GIS maps, Occupant Evacuation Plans, floor plans, etc.). The IRVS plus ISC is the first tool that evaluates risk, is ISC compliant, and provides a uniform and consistent analysis of site conditions and mitigation options.

Using the IRVS Plus ISC

The federal government, through the General Services Administration (GSA) Public Buildings Service, is responsible for over 8,100 leases around the nation. In 2012, the federal leasing process was significantly revised to reduce the number of documents and complexity by using the Standard Request for Lease Proposal, Streamlined Request for Lease Proposal, and Simplified Lease Proposal. All of the leasing documents require a Pre-Lease Physical Security Plan as part of the offer. GSA uses the ISC Physical Security Criteria, and in October 2012, GSA and the Federal Protective Service (FPS) released a new physical security site market survey process to be used to complete the leasing offer.

In practice, the IRVS plus ISC is likely to be used as a collaborative tool, but with different analysis objectives. For GSA, FPS, and the tenants, the tool can be used to define the Existing Level of Protection (LOP) and support the development of the Pre-Lease Building Security Plan and Security Unit Price List. For the owner/property developer, the tool can be used in the same manner as the government, but provide the offeror with mitigation alternatives and costs to make a proposal determination. For local governments, the tool can be used to understand the impact of a federal lease on the retail, residential, and commercial tax base, as

(Continued on Page 13)

[1] More information on the IRVS and related publications and tools from the DHS S&T RSD program are available at www.dhs.gov/bips.

(Continued from Page 12)

well as space utilization. In many cases, such as a large federal lease with a Facility Security Level (FSL) 3 or 4, or where the federal government leases the majority of a building, the requirements for parking and lobby control, restrictions on ground level retail, etc. are contrary to local economic development objectives.

One local government making use of the IRVS Basic and the IRVS plus ISC is Arlington County, VA, a 26 square mile dense urban environment with a significant federal presence that has a substantial impact on the county's economy. Arlington County is interested in understanding the impact of:

- Turnover & recruitment of federal workers
- Environmental sustainability and green buildings, including the effects of sprawl
- Infrastructure and levels of service, especially transportation options and costs
- Security standards and their consequences

To help it evaluate these impacts, the county is using the IRVS Basic for Buildings and the IRVS plus ISC analyses to provide recommendations on how to:

- Determine optimal locations for federal tenants
- Determine the security profile by building and impacts on BID objectives (mixed residential, retail, commercial)
- Determine desired percentage of federal lease per building
- Determine impacts on other CI and business
- Coordinate first responders and in-building access
- Determine tax impacts of each lease
- Determine alternate resilience and redundancy mitigations

In 2012-2013, Arlington Economic Development used the IRVS and conducted a site survey and analysis of the federal commercial lease space, and found there were eight FSL 1, four FSL 2, thirty-three FSL 3, and fourteen FSL 4 sites in the county. Overlaying the FSL sites on the County Master Plan provides insight into which submarkets can provide the desired level of security with minimal impact on the public space, mixed retail and commercial use, and tax base. The IRVS was then used to prepare a baseline assessment of leases that were expiring, or new prospectus leases being issued, and develop the county position for security improvements that would best support the property owners and county's negotiation position.

These are just a few examples of how the IRVS tools are being used in the federal government and by a local municipality. Currently a wide range of federal, state, and local government agencies and private sector organizations are making use of these unique tools available free of charge from DHS to help analyze risk and resilience to improve the safety and security of buildings and their occupants.❖

** To obtain a copy of the IRVS plus ISC module or other information on IRVS and any of its modules, contact Roger Grant (rgrant@nibs.org), Project Manager for DHS projects at the National Institute of Building Sciences.*

The Snowden Train Wreck: Reconsidering 9/11 Imperatives and the Role of Technology

by Michael P. Jackson, former Deputy Secretary, U.S. Department of Homeland Security (2005-2007) and U.S. Department of Transportation (2001-2003)*

More than a dozen years later, public and private sector organizations globally are still grappling to absorb bitter lessons from 9/11. Among the most important is the imperative to improve coordination and interoperability within and among federal, state, and local agencies and with businesses that own and operate critical national infrastructures.

As the morning events unfolded on 9/11, emergency responders in New York could not communicate effectively with each other, nor share critical operational intelligence. Communication among federal, state, and local agencies in a timely manner to mobilize resources was unbelievably rudimentary. Outreach to the owners of critical infrastructure assets was tortuous. For several days at the U.S. Department of Transportation, for example, Secretary Norm Mineta was reduced to communicating with airline CEOs every few hours via non-secure telephone conference calls simply to gain an understanding of unfolding events and their consequences.

Before the attacks, institutional silos made "connecting the dots" about the pending attack unreliable. Guys taking flying lessons who were disinterested in the details of landing safely failed to trigger alarms.

The initial years after 9/11 brought rapid change and meaningful improvements in interoperability. The primary challenges were threefold: *institutional*—establishing necessary policies, protocols, and operational discipline; *technological*—creating tools that make seamless interoperability possible; and *financial*—because implementing what works is costly.

The institutional issues were and still are the thorniest challenge. On the other hand, technological advances made information sharing easier and faster. Moreover, in the early days there was a powerful, largely bipartisan will to invest in what was necessary.

The quantity and quality of intelligence and operational data shared among public sector agencies and with critical infrastructure owners and operators grew quickly. Mining data about potential attackers made the country safer. The institutional structures needed to manage interoperable risk management grew apace, albeit not always perfectly. In short, the imperative to improve communications and operational coordination yielded meaningful progress.

Today however, momentum has slowed, due in no small part to a general *terrorism fatigue*. In the United States, the war on terror has become a distant memory for too many. In fact, it has become somewhat politically incorrect even to speak of a "war on terror."

The Edward Snowden revelations make matters immeasurably worse.

Whistleblower or traitor? Regardless of your view, it's evident that his disclosures have provoked a public policy train wreck. They imperil further progress regarding interoperability. The disclosures have already fundamentally altered the debate about whether and to what extent technology can be effectively harnessed to improve security and diminish risk. In a world saturated with increasingly complex technologies that aggregate and utilize enormous amounts of data for commercial purposes, technology itself is now, for some, suspect altogether when placed in the hands of public sector agencies.

Mistrust of public institutions has consequences well beyond impacts to intelligence gathering and international relations. Such mistrust undermines the networks of cooperation that have been established since 9/11 between the public sector and commercial enterprises, particularly among firms that own and operate critical infrastructures. This web of interdependencies is built foremost on trust and transparency. That

(Continued on Page 15)

(Continued from Page 14)

trust enables real-time sharing by the commercial sector with public sector agencies of information about threats, vulnerabilities, and consequences regarding potential terrorist attacks and other criminal activities.

One technology that facilitates essential interoperability for homeland security is a relatively new software tool known as Physical Security Information Management (PSIM). It is a transformational command center platform increasingly used in the Unites States and around the world by law enforcement agencies, the military, ports, airports, transit systems, and many other civilian agencies, as well as by corporations large and small. It continuously fuses, instantly correlates, and effectively converts vast amounts of data into meaningful and actionable information gathered from virtually any type, brand, or generation of physical security system or sensor—and from many other networked management applications. Deployments often integrate large numbers of security cameras, video recorders, access control systems, intruder detection systems, fire alarms, Computer Aided Dispatch systems, bollards, radars, and other more exotic or specialized sensors and applications.

PSIM helps link multiple organizations—often those with geographically dispersed assets—and provides enhanced capabilities to manage risk in a more cost-effective, efficient manner. Each participating organization decides what to share and when to share it. PSIM can automate responses when seconds matter most. It works in concert with other security tools that are breaking new ground in risk management. These include sophisticated video analytics, shot detection and location technology, crowdsourcing analytics, the capacity to merge fast-breaking intelligence with industrial controls, and asset management systems that instantly adjust risk posture to risk profile.

For large-scale public events, such as the Boston Marathon, private institutions have collaborated with public agencies to share data effectively. For instance, the bombers at last year's marathon were identified on a video feed from private cameras owned by a local retailer. We seem to face almost weekly incidents such as shootings in malls and cyber-attacks or other disruptions aimed at commercial enterprises. The case is strong for more collaboration, where private sector assets—particularly video feeds covering public spaces—may be shared with public safety partners for special events to enhance safety and security.

Against this backdrop of increased capability and need, the Snowden disclosures have unleashed an almost atavistic distrust of technology in some circles, a mindset that can undermine the homeland security mission. We live in an ugly world of risk. Technology harnessed properly makes reducing such risk possible. It requires, however, the alignment of what is technologically possible with our nation's fundamental rights and principles of fairness.

In the months ahead, our success in the post 9/11 era is once again disproportionately in the hands of policy makers, both public and corporate. A respectful balance can be struck, and must be sustained. Rather than being the locus of a threat to privacy, emerging technologies can actually structure and make effective such a balance. Indeed, technology properly used can shift the balance point toward protecting individual freedoms, if properly embraced.

However tragic, actual train wrecks do tend to generate introspection, greater safety, and important lessons learned. As with the early months following 9/11, once again this moment demands clear-thinking, bipartisan leadership, and calm debate about what is at stake here and abroad.❖

**Michael P. Jackson is Chairman and CEO of VidSys, Inc., a leading supplier of PSIM software. He has worked in the public sector for three presidents, at the White House, and at three federal Departments. In the private sector, Jackson has been a Director or senior executive with large and small corporations in the transportation and security industries.*

Force Multipliers and the Terrorism Planning Cycle

by Jeff Zisner, President & CEO, AEGIS Security & Investigations*

As a professional security expert, I am often asked how to prevent terrorist bombings, active shooters, and other terrorist attacks. Disrupting an attack during the planning process and hardening a target must both occur to successfully prevent and defend against an attack. Terrorist attacks do not just come together overnight. The planning process, depending on how intricate the attack is, may last weeks, months, or even years! It is universally accepted that terrorists move through terrorism pre-incident indicators to plan and deploy an attack. In order to prevent a terrorist bombing, much like the Boston Marathon attack, recent school violence, or mall shootings, law enforcement needs to work with information provided by an educated public. Those individuals properly trained to recognize and report suspicious behavior are known as force multipliers.

When tasked with developing a force multiplier program, one should first reference various government and non-profit approaches. FEMA developed the Community Emergency Response Team (CERT), the FBI developed Infragard with the Infrastructure Liaison Officer and Terrorist Liaison Officer programs, and local law enforcement like the Los Angeles Police Department created citizen's academies. These organizations and the programs they run are successful because they create relationships with loosely affiliated groups of people to aid the sponsoring organization's mission. Across the country, businesses can benefit from utilizing government resources and working with a consultant to establish their own robust security training programs.

These ideas can effectively be applied at commercial facilities such as hotels, retail outlets, office buildings, and entertainment venues just as well as schools and colleges, both public and private. Successful security and threat awareness programs cross-train employees working in unrelated specializations in pre-incident indicators as well as reporting, mitigating, and responding to threats. This training is typically designed and presented by local law enforcement, security professionals, or risk managers. Whether they are human resources managers, sales staff, operations, or support staff, these individuals can quickly become additional eyes and ears, extending the reach and effectiveness of a safety and security program. The core of the force multiplier program is training individuals in the pre-incident indicators so that they know what to look for, and how to report it.

There are seven potential steps or phases in which citizens can assist in preventing terrorist attacks, many of which specifically relate to commercial facilities. The first step involves recognizing when surveillance is being performed. This involves distinguishing between a tourist and someone looking at the physical security of a site, traffic patterns, or how an event is being set up and executed. The number one line of defense is public citizens notifying law enforcement of people and/or their actions that seem out of place. This information should be given to local law enforcement, or the local fusion center (a joint intelligence center designed to receive and investigate tips and leads).

The second step to prevent a terrorist attack is understanding how terrorists use elicitation to extract information. Terrorists speak with anybody with insider knowledge about a potential target. It could be a front desk person at a hotel, a facilities manager, or a janitor. The purpose of elicitation is to obtain information that cannot be found elsewhere. It may include shift changes, policies and procedures, or even something as simple as asking when things are busiest. Distinguishing between a curious visitor and a potential terrorist can mean the difference between thwarting an attack and becoming a victim.

The third step involves stopping tests of security. A test of security is not a dry run or a trial run. A test of security is designed to observe response time, see how far someone

(Continued on Page 17)

(Continued from Page 16)

can go in to a restricted area, or to obtain information on procedures. A terrorist successfully testing security means he or she can now start to put the plan in to motion. Individuals caught testing security should be held for questioning both by the site personnel and by law enforcement. The information obtained will be added to a database of other incidents and identifiers and could be linked to other similar instances.

The fourth step is to minimize the funding of terrorist operations. Terrorism is expensive. Operatives have to pay for a base of operations, food, equipment, transportation, etc. Typically, terrorists are involved in fraud, theft, narcotics, or other crimes. If you witness a large transaction done in all cash or gift cards, it could be a sign of a potential terrorist attack being planned. Write down a description of the individuals involved, what vehicles they were driving, when and where it happened, and exactly what you observed. Report this information to law enforcement.

The fifth step for successful prevention is to stop terrorists from acquiring supplies. Typically, retailers must pay special attention to their employees' training. Something as simple as seeing an unusual group of supplies or chemicals being sold and asking the purchaser to wait for a manager may do the trick. Any suppliers selling items that could be used in an attack should have tripwire training programs to prevent such sales from taking place.

The sixth step is recognizing suspicious persons. If the presence of an individual seems out of place, report it to law enforcement. These folks may be genuinely lost or in need of assistance—or preparing for an attack.

The seventh and final defense in preventing a terrorist attack is to stop it during a dry run. If a dry run is successful, terrorists may then be fully prepared to carry out a terrorist attack. If you observe what you think may be a dry run or are in the midst of an attack, immediately call 911.

It is important to remember that anything or anybody that seems out of place, no matter how potentially insignificant, should be reported to law enforcement. Infragard is a partnership between the FBI and the private sector designed to provide training and information sharing to public stakeholders. For more information on pre-incident indicator training, and to join Infragard, visit www.infragard.net.❖

** Jeff Zisner is President & CEO of AEGIS Security & Investigations, a Certified Protection Professional, a 9 year veteran of the industry, and Commercial Facilities Sector Coordinator for the FBI's Infragard Members Alliance of Los Angeles. He regularly provides security consulting, penetration testing, and training services for corporate and public clients in addition to security services and private investigations. He can be reached at 310-838-2787 or by email at info@aegis.com.*

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University 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