Brick by Brick

Border wall plans continue to take shape alongside overall efforts to better secure the country’s southwest flank

Also Inside:

Platform Preferences
Jihadis thrive on ‘Telegram’ app’s versatility, making it a top online terror tool

Collective Palpitations
European nations must come to grips with a president who does what he says he’s going to do

Fluid Terrain
Vast Coast Guard responsibilities test limits of US reach for maritime border defense
DEPARTMENTS

2 UPDATES & RESPONSES
Considering Airport Insider Threats, Cyber Intruders and Perimeter Security
By Anthony Kimery

3 EDITOR’S LETTER
Vacancies, Placeholders, Morale Take Center Stage at DHS
By Anthony Kimery

4 OPINIONS & POLITICS
CBP Ignores Mandate Under 2006 Safe Port Act
By Jim Giermanski

7 BORDER SECURITY
DHS Feeling Pressure to Improve Biometrics Program
By Sylvia Longmire

8 AGENCY SPOTLIGHT
DEA Relies on Multiagency Collaboration in Drug Smuggling Fight
By Krysta Dodd

10 EMERGENCY PREPAREDNESS
21st Century Information Sharing and Communication Requirements Pose Significant Challenges
By Sam McGhee

12 CYBERCOM
Cybersecurity Takes Pages from Swiss Bank Playbook
By Mike Baker

14 ACADEMIC INSIGHTS
Homeland Security Studies React to New Administration
By Godfrey Garner

16 GLOBAL WATCH
News from Around the World
By Dave Sloggett

18 INDUSTRY NEWS
Industry Roster

44 TOOLS & TECHNOLOGY

47 RESOURCES
Advertiser Index

48 GROUNDBREAKERS & POWERHOUSES
George Zoulias, President, CEO and Founder, Perfecta Federal

PHOTOS COURTESY OF CBP, COMPOSITION BY JOHN FORADARIS

JOIN THE DISCUSSION
Considering Airport Insider Threats, Cyber Intruders and Perimeter Security

Homeland Security Today reported in February that the House Committee on Homeland Security majority staff report, America’s Airports: The Threat From Within, found the majority of the nation’s airports do not have full employee screening at secure access points, resulting in a serious insider threat vulnerability, and “are unable to demonstrate the security effectiveness of their existing employee screening efforts, which consist largely of randomized screening by Transportation Security Administration [TSA] officers or airport law enforcement personnel.”

Disturbingly, the report noted that the Department of Homeland Security (DHS) inspector general revealed in 2015 that “73 aviation workers with links to terrorism were either currently or recently employed at airports across the United States with access to secure and sterile areas,” and that, “[s]ubsequent oversight efforts revealed that while TSA reviewed each individual and determined whether they were a threat to aviation security, the agency had missed terrorist ties due to a lack of access to certain data sets held by other entities within the US government. Despite longstanding efforts to be granted access to additional intelligence databases, DHS and TSA were met with resistance and delay by other federal agencies.”

The Government Accountability Office (GAO) had already noted in an audit report that TSA officials have long acknowledged the potential threat from airport workers, but deemed the threat a “known and accepted risk.”

In response to the Homeland Security Today report, Arbor Networks Chief Security Technologist Darren Anstee told Homeland Security Today that, “While the Homeland Security Committee report focuses on the physical security risks posed by the ‘lone wolf’ insider threat at American airports, it is important to note that there is also a significant insider threat cyber risk.”

Anstee explained that, “Many organizations have focused their cybersecurity at the perimeter of their networks to stop bad actors getting in. While this is important, many are blind to what goes on within their infrastructures. This is a key problem which is illustrated by previous leaks of classified data where insiders have been seen to hoard, and then extract, large amounts of data while remaining undetected. Data thefts are one thing, but imagine the ramifications this can cause at airports. If an air traffic control system, or even just an airline check-in system was targeted by an insider intent on disrupting system continuity, there would be wide-spread disruption, costing the economy millions of dollars and causing major inconvenience – and possibly personal risk to many travelers.”

Anstee said, “It is becoming increasingly imperative for organizations to instrument the interior of their networks so that they can see what is going on everywhere, so that they can detect suspicious or malicious behavior quickly wherever it occurs. This is not easy for large, geographically distributed sites with many terminals of different types – like airports – unless the network is harnessed to provide the necessary visibility. The network is the conduit for all inter-device communication, and thus can be harnessed for pervasive visibility. Internal network analysis has become a key part of the fight against cyber-criminals in the enterprise space, and this kind of monitoring needs to be mandated in areas critical to national security – such as transport hubs, utilities etc.”

Meanwhile, new video analytics software designed to provide advanced analytics and generate real-time alerts designed with government entities such as airports, can alert to intrusion detection, left-behind object detection, facial recognition and camera tampering alerts. All of these technologies serve as a security force multiplier.

These technologies are vital. John Halinski, a former TSA deputy administrator and former chief operating officer for TSA, warned in his Homeland Security Today report, “Curbside Vulnerability,” about the lack of security outside and immediately inside the nation’s airports.

“The street side of an airport historically has been susceptible to attack by terrorists, and this vulnerability is now being exploited,” Halinski said, adding however, “Unfortunately, this zone from the front of the airport to the federal checkpoint is many times a ‘no-man’s land’ lacking any real security personnel, adequate physical protective structures, a general lack of security technology and effective coordinated security policies.”

– Anthony Kimery, Editor-in-Chief
First responders in the 21st century increasingly face multifaceted active threat scenarios. The complexity of recent national and global attacks, as well as the potential of extreme natural disasters and weather emergencies, challenge those charged with saving lives and ensuring the best possible outcomes during these events more than ever.

While the challenges seem more complicated and potential outcomes more intense, there is a dichotomy between required response and available resources to manage these types of events. On one hand, post-9/11 state, local, federal and private sector entities are expected to work together during preparation and cooperate fully during emergency response. Obvious complications emanate from these relationships, as they represent multiple disciplines and jurisdictions. Related issues regarding their respective structures may be incompatible as well. On the other hand, technology has advanced and relationships have been created or improved to meet these uncommon demands. In addition, there are many agencies and jurisdictions who’s after-action reports offer key information through improvement matrices that would serve any jurisdiction in planning for a potential emergency or an attack. Planners must take advantage of these resources in the earliest stages of planning.

Today’s Challenges

Due to the nature of social media, governmental organizations may be exposed more quickly and judged more harshly than ever before for decisions made during crises. There is a heightened awareness of emergency management responsibilities and results produced within American culture. Social and mass media reports can quickly influence public sentiment.

Further, the characteristics of an active shooter or terrorist attack can include multiple, simultaneous attacks on soft targets in a large geographic area. This can swiftly evolve into a multijurisdictional cross discipline and rapidly developing threat requiring real-time information management. In the United States, active shooter cases continue to increase in frequency and complexity. Constantly morphing methods among attackers put emergency plans and procedures to the test. This requires leaders to be resilient in assessing dynamic threat environments and quickly and effectively shifting priorities. How? By ensuring information is collected, analyzed and distributed rapidly. Leaders will be judged on how they respond to such complex environments, and given the predictability of an unpredictable scenario occurring, the public pressures of crisis decision-making will be in the forefront.

The previous barriers created through silo-thinking between agencies and disciplines have softened significantly since 9/11. Pre-event information sharing is a much-improved realm, with the increase in joint intelligence bulletins disseminated to state and local agencies from the FBI, Department of Homeland Security and others. With the advent of fusion centers and their ability to serve as central clearing houses of information pertinent to local constituents while coordinating with national information-sharing resources, the first responder community can rely on this aspect of information sharing as a basis for awareness and preparation. This, however, does not necessarily solve the challenge of the need for situational awareness or understanding rapidly morphing threat dynamics in each incident.

Critical Need for Immediate Planning

Pre-event planning for dynamic threat scenarios has taken on emerging features. It may have been sufficient at one time to plan, train, equip and exercise emergency plans intermittently. In today’s environment, while certain facets of a plan may remain more static – such as equipment needs and types – aspects involving information sharing require constant monitoring, updating and maintenance. Technological advances in real-time information sharing offer the opportunity for rapid assessment, allowing rapid decision making among emergency response leaders in adjusting to the threat’s rapidly changing scenario. Examples of these include apps for smartphones, Web-based secured portals for broad-based communication efforts among responder partners during events, social network applications, radio interoperability between disciplines and jurisdictions, to name a few. However, it is essential to begin identifying and establishing these capabilities immediately for these resources to be realized. The common thread among these solutions is to:

1. Establish potential partners (followers, in the case of social media applications) necessary to maximize these modes of information-sharing.
2. Establish common objectives.
3. Create necessary informal or formal agreements to support the understanding and use of such technology.

Established Resources

Post-9/11 efforts have emphasized regionalized approaches to improvements in capability areas where gaps in mitigation, prevention, response and recovery exist. For many communities, funding for resources is scarce; this does not have to remain a constraint. Fusion centers are established in almost every state in the country to serve its communities in crucial information-sharing needs during critical events. The National Network of Fusion Centers is constantly assessing and upgrading ways in which fusion centers communicate with their respective communities. Emergency planners should contact their fusion center directors,
who should have immediate suggestions for connecting to established best practices in information-sharing measures. This may include rapid information-sharing smart phone apps utilized by the fusion center and key partners during emergency incidents.

Further, most fusion centers have some version of a terrorism liaison officer program where local agency representatives are trained, then incorporated into an information-sharing architecture. This creates an expanded network of collection points, which may support real-time information-sharing needs. In addition, the National Network of Fusion Centers has created a real-time information-sharing portal on the Homeland Security Information Network. This secure chat forum was created after some of the more notable active shooter attacks: The Century 16 shooting in Aurora, Colo.; the Sikh temple shooting in Oak Creek, Wis.; the Clackamas Town Center shooting in Portland, Ore.; and the Sandy Hook school shooting in Newtown, Conn. This capability allows fusion centers to communicate in real time about facts and circumstances of a given incident, manage tips and leads, and coordinate information-sharing partnerships among fusion centers in contiguous states – including sharing analytical and intelligence product capabilities.

Today’s emergency management and first responder planners are challenged more than ever to effectively plan and execute emergency response measures for the myriad of rapidly developing and dynamic threats. Often, these threats cross jurisdictional borders and require multiple disciplines to respond to the incident. Central to this critical planning is the need for real-time situational awareness and information-sharing. To accomplish this requires pre-establishing alliances, intergovernmental agreements and multilayered, redundant communication methods. While the challenge may seem daunting, the solutions to these issues can be found among agencies who have dealt with these incidents and implemented methods to improve their short-comings. Leveraging lessons learned from past events can significantly reduce a planner’s learning curve, and the methods may be of little or no cost with effective pre-planning. 

A lieutenant with the Aurora, Colorado Police Department, Sam McGhee currently is the Professional Standards Section/Emergency Services Coordinator. For two years he served as deputy executive director of the Colorado Information Analysis Center and served a one-year fellowship with the Interagency Threat Assessment and Coordination Group located in the National Counterterrorism Center in Washington, D.C. In 2015, he helped create the implementation plan for the National Network of Fusion Centers. He’s also a member of the Committee on Homeland Security for the International Association of Chiefs of Police.