domestic preparedness .com

DomPrep Journal

US Annual $100 Volume 9 Issue 7, July 2013

CYBER


THE UNTHINKABLE HAPPENED
WHAT'S NEXT?
SALAMANDER
WHEN IT MATTERS
When the unthinkable happened in Van Buren County, Arkansas,
Salamander was there. Click below to learn more.
FIND OUT MORE | TALK TO AN EXPERT
Salamanderlive.com/VanBuren | 877.430.5171

Business Office
517 Benfield Road, Suite 303
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

Susan Collins
Associate Publisher
scollins@domprep.com

James D. Hessman
Editor in Chief
JamesD@domprep.com

Catherine Feinman
Editor
cfeinman@domprep.com

Carole Parker
Customer Service Representative
cparker@domprep.com

John Morton
Strategic Advisor
jmorton@domprep.com

DomPrep Journal is electronically delivered by the IMR Group Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

Articles are written by professional practitioners in homeland security, domestic preparedness, and related fields. Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher. Text is the opinion of the author; publisher holds no liability for their use or interpretation.

IMR GROUP

Editor's Notes

By James D. Hessman

As cyber threats increase, so do the costs to counteract such threats. The ten knowledgeable authors in this month's printable issue of *DPJ* take a long look at CYBER – the weapons, the security, the capabilities, and other tools and technological progress.

Monica Giovachino and Sarah Tidman lead off with a persuasive discussion of how important it is that the United States continues to expand its own cyber capabilities. Such efforts have become increasingly important not only in everyday business operations but also in the emergency planning needed by forward-deployed U.S. naval/military forces throughout the world and by all levels of government.

Markus Rauschecker spells out some of the domestic particulars in greater detail in his analysis of how cyber systems have quickly become the most essential tool used by emergency managers, at all levels of government, to cope with floods, earthquakes, and other major disasters – both natural and manmade. Armond Caglar follows up with a report on the high cost ($300 billion per year, and going up) – to U.S. businesses and taxpayers – that has already been lost to foreign hackers, and warns that a "holistic intelligence program" is urgently needed to protect both business and military secrets from even greater losses in the near future.

Communication and transportation are also critical during every disaster. Glen Rudner points out that lives also are at stake, and uses the Boston Marathon bombings to illustrate how an entire city can be, and in this case was, shut down by one major and malicious incident. Joseph Cahill uses Block Island (not too far from Boston, coincidentally) as a best-case example of how even a relatively isolated community can help itself with hard work, advance planning, and some quick mutual-aid assistance from other communities.

Joseph Trindal shifts to a macrocosm approach with his article on how Washington, D.C., and its closer-in suburbs are joining the forces of its private sector to help protect the entire National Capital Region by joint planning, joint exercises, and joint operations. Raphael Barishansky focuses special attention on the whole-of-community approach recommended in the federal government's National Preparedness Report, which: (a) comments favorably on the outstanding efforts made by New Jersey and New York in coping with Hurricane Sandy; but (b) recognizes that major improvements are still needed in other areas of immense importance (nursing homes, for example) during times of sudden disaster.

Sheri Donahue focuses much needed attention on the hard-working, knowledgeable, and essential professionals known as subject-matter experts (SMEs), and uses that as the firm foundation needed for the rapidly growing InfraGard community of cyber experts who have joined forces, and combined their individual talents, in every region, state, and major city throughout the entire country. Rodrigo Moscoso rounds out the issue, in a most unfortunate as well as most timely manner, with his report on: (a) this year's DEF CON conference; (b) the increasingly helpful private sector/federal government working relationships developed and nurtured at previous DEF CONs; and (c) the potentially disastrous effect on those relationships, at this year's conference, caused by the so-called "PRISM" revelations.

About the Cover: With an eye on security, public and private stakeholders are making efforts to guard proprietary information, to prevent hackers from accessing code and other valuable data, and to communicate and coordinate efforts. This inspired combination was created by Susan Collins, who combined two iStock photos to represent both the cyber threat and the solution.

DomPrep Writers

Raphael M. Barishansky
Public Health

Joseph Cahill
EMS

Craig DeAtley
Public Health

Kay C. Goss
Emergency Management

Stephen Grainer
Fire/HazMat

Rodrigo (Roddy) Moscoso
Law Enforcement

Corey Ranslem
Coast Guard

Glen Rudner
Fire/HazMat

Richard Schoeberl
Law Enforcement

Dennis R. Schrader
CIP-R

Joseph Trindal
Law Enforcement

A Roadmap for Improving Cyber Preparedness

By Monica Giovachino & Sarah Tidman, Cyber & IT

Cybersecurity has become one of the nation's most serious challenges today. As a top priority of the White House, many initiatives are underway to ensure that the nation's critical infrastructure and networks are protected. Nonetheless, the role of emergency managers in preventing, mitigating, and responding to a major cyber incident with physical consequences remains unclear. In fact, according to the U.S. Department of Homeland Security's 2013 *National Preparedness Report*, cybersecurity is still one of the lowest-rated capabilities in the State Preparedness Report – and many states have reported that they do not expect to focus on building additional capacity in this field. This is despite the fact that findings from the Federal Emergency Management Agency's *National Level Exercise (NLE) 2012 Quick Look Report* pinpointed many areas for improvement specific to a cyber scenario that could adversely affect all levels of government.

Although cybersecurity is traditionally the responsibility of the nation's information security and technology communities, combating cyber attacks that could cause physical consequences is also a shared responsibility that involves emergency managers at all levels of government, law enforcement agencies, the private sector, and other "stakeholders." Moreover, according to participants in a recent Cyber Preparedness Workshop – conducted by CNA's Safety and Security Division on 25 April 2013 – many state and local jurisdictions also lack the mechanisms needed for engaging this diverse community in a coordinated effort. CNA defines cyber preparedness in general as the process of ensuring that an agency, organization, or jurisdiction has developed, tested, and validated its own capabilities to protect against, prevent, mitigate, respond to, and recover from a significant cyber incident.

Because emergency managers play an important role in cyber preparedness, CNA developed a cyber preparedness continuum to provide a roadmap for emergency managers to evaluate and improve their jurisdictions' or organizations' levels of cyber preparedness before, rather than after, an actual cyber incident precipitates cascading physical effects. Similar continuums have been used successfully in other programs, such as interoperable communications, to strengthen capability and capacity.

The cyber preparedness continuum used in the workshop (see figure) consists primarily of the four elements indicated in dark blue: Coordination; Information Sharing; Emergency Planning and Readiness; and Continuous Improvement. The actions described in the light blue boxes indicate increasing levels of preparedness – from left to right across the diagram.

As was strongly suggested by the Cyber Preparedness Workshop discussion – combined with the findings included in the NLE 2012 "Quick Look Report" – the key challenges that emergency managers now face in this field are those identified in each of the following four elements:

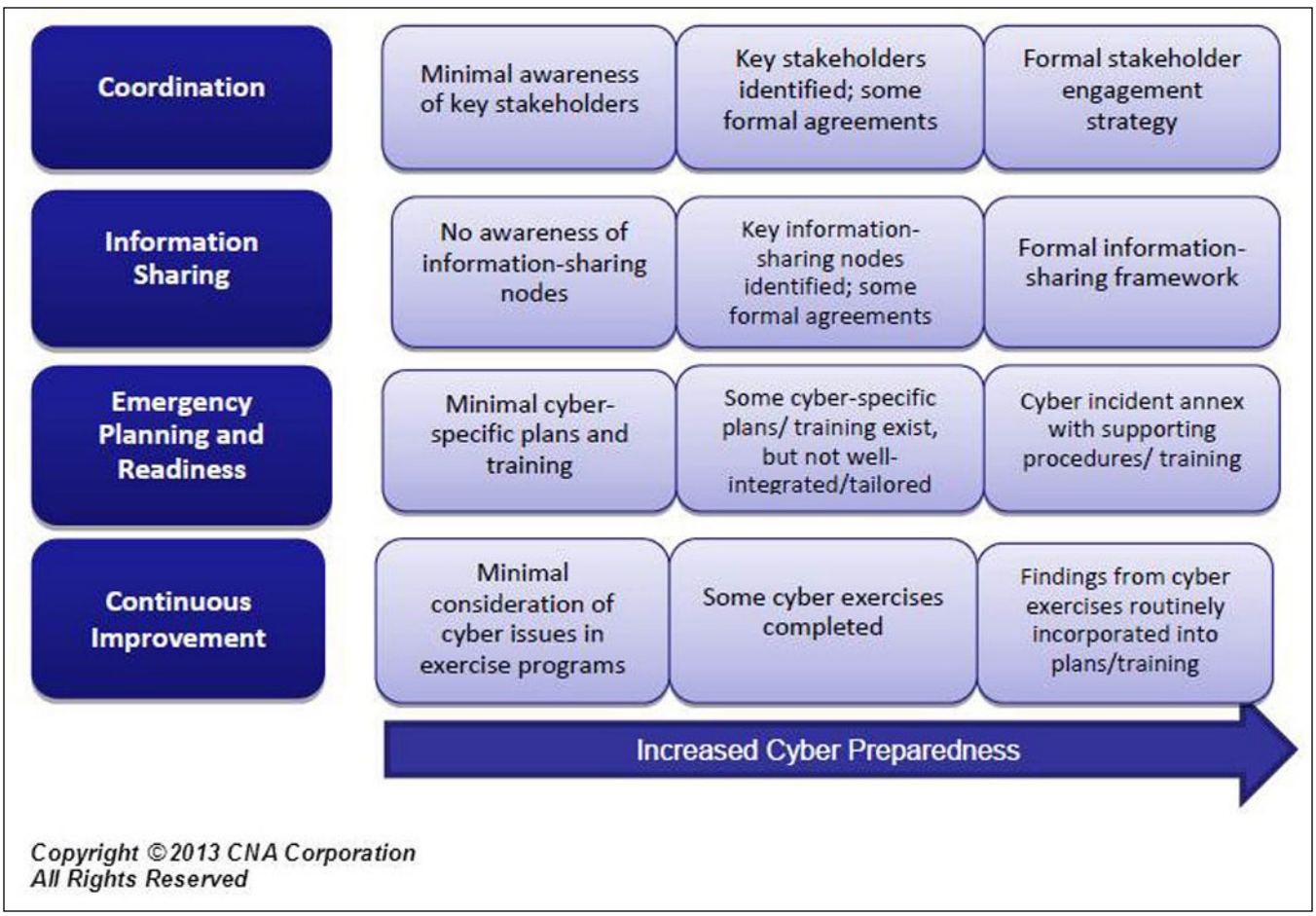
Coordination

At present, there are few incentives for the private sector to coordinate more closely with the emergency management community in cyber preparedness activities. Although developed primarily to promote information sharing as it relates to cyber resiliency, the Western Cyber Exchange – a consortium of businesses, information-technology security professionals, as well as federal, state, and local government representatives – provides one example of how a consortium could help to promote both coordination and information sharing between the private sector, emergency managers, and the other stakeholders involved.

- Although emergency managers need a better understanding of how they integrate into the national response structure both during and following a significant cyber incident, NLE 2012 confirmed the obvious fact that the respective roles of two key elements of the response structure – the U.S. Department of Homeland Security's National Cybersecurity and Communication Integration Center (NCCIC), and the U.S. Computer Emergency Readiness Team (US-CERT) – remain unclear.

Information Sharing

- The notification process for cyber incidents is not well understood by many emergency managers – uncertainties include what types of information should be shared, what agencies should share this information, and what the thresholds for sharing information should be. NLE 2012 revealed that the draft National Cyber Incident Response Plan and the National Cyber Risk Alert Level did not provide sufficient information on: (a) the actions various participants need to take; or (b) the various types of information they need to share.



- Emergency managers lack awareness of how cyber-related data is analyzed to identify – and, therefore, effectively respond to – ongoing cyber attacks across the nation. This finding was confirmed in NLE 2012 when the NCCIC staff had difficulty analyzing and connecting multiple incidents and then producing useful situational awareness products.

Emergency Planning and Readiness

- A critical goal of planning and readiness is the development of a better understanding of the roles played by local networks and systems, the potential impact of a cyber incident on critical infrastructure, and the various interdependencies across and connecting all sectors. Nonetheless, NLE 2012 showed that there is still a lack of consensus regarding the level of cyber threat and vulnerability information that should be shared between the public and private sectors.

- NLE 2012 also demonstrated several planning challenges likely to occur during the response to a significant cyber incident – specifically including: (a) several difficulties in developing viable Incident Action Plans; and (b) a lack of clarity on when and how federal assistance (authorized by the 1988 Stafford Act) could be used.

Continuous Improvement

- The designing of realistic exercise scenarios is a continuing challenge. The cyber exercises carried out to date, in fact, have not always realistically simulated the probable impact of cyber attacks on critical infrastructure, such as power grids.

- Cyber exercise scenarios often do not include cascading physical effects because of the challenges described earlier. Largely for that reason, most current exercises are not as effective as they should be in helping emergency managers understand not only their own local systems and vulnerabilities but also the numerous complexities involved at other levels in a cyber incident.

Identifying current gaps and challenges is a significant first step toward strengthening the United States against

the ever-increasing threat posed by cyber attacks and the physical effects that follow. However, analyzing and dissecting these discussions and translating them into actionable cyber preparedness activities requires a great deal of resolve and determination from a diverse set of communities as well as effective leadership on the part of emergency managers. In summary, it is only through deliberate, cyber-focused planning activities, followed by continuous assessments and improvements, that the nation as a whole can better protect its critical infrastructure systems – and, therefore, the overall safety of the American people.

Monica Giovachino (pictured) is a managing director in the Safety and Security Division at CNA, where she has been employed since 1994. She has special expertise in the design and evaluation of complex exercises and in the evaluation of real-world events. She also has: (a) led the evaluations of a number of "TOPOFF" (Top Officials) Exercises and National-Level Exercises planned and carried out for the U.S. Department of Homeland Security; (b) managed numerous other exercise programs for various local, state, and federal agencies; and (c) led the analyses of several complex real-world operations. Included in the latter category were evaluations of responses to hurricanes, disease outbreaks, chemical/biological "events," and law enforcement incidents.

Sarah Tidman is an associate research analyst in CNA's Safety and Security Division. Her work there has focused on emergency management and preparedness. She has special expertise in the design and evaluation of both training exercises and real-world events; has led and assisted in the analysis of many local, state, and federally sponsored exercises; and has deployed to observe and evaluate response operations during real-world incidents. In one of her most recent projects, she co-led the national evaluation for the Federal Emergency Management Agency (FEMA)/ National Exercise Division's (NED) National Level Exercise (NLE) 2012.

When Cyber Space Meets the Real World

By Markus Rauschecker, Emergency Management

Although many Americans may reasonably assume that the federal government will handle the response to most cyber incidents, the reality is often quite different. During a conference held at Georgetown University in April 2013, Michael Daniel, cybersecurity coordinator at the White House, suggested that the emergency management model be applied to cope with most cyber incidents. Adoption of this approach would generally dictate that the responses to most such emergencies would be managed primarily at the local and state levels, unless authorities at those levels are unable to adequately respond.

If the emergency management model is applied, the responsibility for dealing with a cyber incident would fall principally on local authorities. Therefore, they must ensure that they are adequately prepared to cope with such incidents within their own jurisdictions.

For all types of emergencies, the success of the response depends not only on the practical expertise and capabilities of the first responders, but also on their ability to work together effectively. In dealing with cyber incidents, local and state emergency responders must also have strong working relationships with their information technology (IT) counterparts. Currently, those relationships often either do not exist or need to be reinforced. If the responsibility of managing a cyber incident falls primarily on them, then local and state jurisdictions must find better ways of establishing the necessary relationships between and among their own emergency managers and IT professionals. Doing so would ensure effective responses to an ever-increasing threat.

Managing Cyber Threats: COOP Planning & Cooperative Skills

The technical aspects of a cyber incident may tempt at least some emergency managers to hand off the response efforts to the IT professionals involved. In that context, however, it is important to consider Daniel's assertion – at the Georgetown conference mentioned above – that a cyber incident may be managed in ways similar to those applicable to any other type of emergency. This approach would be particularly true considering the fact that real-world power outages, traffic disruptions, and/or critical infrastructure failures could possibly result from a single attack within cyber space.

Basic emergency response principles should not be neglected when faced with a cyber incident. The Incident Command System (ICS) is still applicable when coordinating a response to a cyber incident. Continuity of Operations (COOP) planning also is vital when a cyber disruption occurs. Well-designed COOP plans not only are applicable to all types of hazards, but also will allow the organizations and agencies involved to continue their essential functions during any type of emergency. In that context, it is irrelevant with respect to the COOP plan if an IT system outage was caused by a natural disaster, a power outage, or a cyber attack – because the plan itself would define the backup capabilities that will be needed until normal operations can be restored.

The most important distinction, however, between cyber incidents and other types of emergencies lies in the technical expertise required to recover from the incident and to restore normal operations. The response to and/or recovery from a cyber incident would be nearly impossible without the collaborative skills and services of: (a) IT professionals to provide the technical expertise required to recover and restore the systems directly affected; and (b) emergency managers to coordinate the response and deploy the human and material resources needed to achieve that goal.

Without clearly defined roles and expectations, it would be difficult for emergency managers and IT professionals to coordinate their efforts. Although IT professionals may have developed and promulgated robust data and system recovery plans, they nonetheless may be unaware of certain emergency response principles related to ICS and/or continuity planning. Similarly, emergency managers often do not possess the technical expertise needed to understand the requirements and procedures postulated for restoring IT capabilities – and, therefore, may have unrealistic expectations as to the probable recovery time.

Bringing Together All the Pieces

The first step toward bridging the current gap between emergency managers and IT professionals is to engage them in joint training. Programs such as the Federal

Emergency Management Agency's Resilient Accord Workshop, which addresses emergency management and continuity planning considerations in response to cyber incidents, are immensely helpful. One of the principal goals of the workshop is to bring together emergency managers and IT professionals to establish and/or enhance the working relationships between the two disciplines. By better informing each side about the other's roles, responsibilities, and capabilities, emergency managers themselves will become better equipped to coordinate the response – and the IT professionals involved will become more fully integrated into the response.

Fortunately, some U.S. jurisdictions are already going a step further and actively encouraging such collaboration. A number of New England states, for example, have established "Cyber Disruption Teams" consisting of representatives from the emergency management, information technology, and public safety communities. These teams are deployed with members who have not only been cross-trained but also have: (a) completed introductory courses on incident command and information risk management; and (b) gained practical experience through workshops similar to the FEMA Resilient Accord. These training sessions help familiarize team members with emergency management and IT concepts so that, during future responses to a cyber incident, all parties will use the common terminology and possess the same understanding of the sometimes complex issues involved.

By working more closely with the IT community and developing more effective working relationships, emergency managers will gain a clearer understanding of not only the extent and ramifications of the incident, but also of the human and material requirements and resources needed for a successful recovery. In short, a mutual understanding must be developed and sustained in every local jurisdiction throughout the nation to effectively prepare for, respond to, and recover from cyber incidents. The success of any emergency response is founded on the same type of strong relationships.

Markus Rauschecker is a Senior Law and Policy Analyst for the University of Maryland Center for Health and Homeland Security (CHHS). He joined CHHS in March 2008 and currently serves as Staff to the National Capital Region (NCR) Senior Policy Group. He also served as the lead planner for the District of Columbia's Continuity of Operations program, and worked on two Presidential Inaugurations, providing both management and operational support. He earned his BA from Georgetown University in 2002 and received his JD from the University of Maryland School of Law in 2006. He is admitted to practice law in the state of Maryland.

Holistic Security – Various Ways to Reduce Vulnerability

By Armond Caglar, Cyber & IT

According to a May 2013 report of the Commission on the Theft of American Intellectual Property – an independent, bipartisan initiative of U.S. representatives from both the private and public sectors – the theft of intellectual assets is estimated to cost U.S. businesses more than $300 billion annually. Increasingly, U.S. companies are not only facing persistent threats to the integrity of their business activities, but also grappling with the need to stem the erosion of their companies' values caused by commercial espionage carried out by both foreign and domestic actors.

In addition to the harm caused to the businesses directly affected, such thefts also contribute to a significant loss of U.S. jobs and a corresponding decline of the national economy in terms of a reduced gross domestic product. In some cases, the thefts also have resulted in the loss of U.S. ingenuity to rivals who are not only stealing intellectual property but also counterfeiting and/or otherwise adapting that property to foreign markets by focusing on low-cost positioning and mass consumption – both of which subsequently evolve into market disruptions in their own right.

These challenges have been not only costly but also fairly consistent in recent years. According to the 2012 Cost of Cyber Crime Study of 56 U.S.-based companies (many of them multinational corporations) – sponsored by Hewlett-Packard and carried out by the independent research group Ponemon Institute – cyber espionage attacks have increased by an average of 38 percent from 2010 to 2011. The average annual cost for the companies included in the 2012 study amounted to approximately $8.9 million. Moreover, the World Intellectual Property Organization headquartered in Geneva, Switzerland, estimated that, "In 1998, intangible assets constituted 80% of the value of Fortune 500 companies." Obviously, the potential for truly extraordinary losses in the foreseeable future is not only evident but also probable.

Protecting U.S. Companies From Cyber Threats

Although investments in protective measures such as firewalls and/or anti-virus solutions are popular options, they are insufficient in isolation. In an age of sophisticated and frequent attacks, particularly as related to the state-sponsorship of intellectual property theft through cyber and insider threats, private firms – the U.S. government as well – must ensure that security investments are diversified throughout their entire business plans and operations.

Diversification does not necessarily mean, though, that security investments in specific components of an enterprise do not provide protection. They certainly can, and often do. The problem is that securing individual components does not secure the business as a whole. Some software vendors may purport to sell their products as the one and only "cure-all" needed for total security and protection. But new technology added to a company's existing security infrastructure creates additional complexity. One likely result is that at least some of the company's data may not be properly analyzed and correlated with other data that the same firm creates.

Application behavior, system performance, user actions, and deceptive activity are all critical data streams that can serve as invaluable intelligence in any post-incident investigation – or, preferably, pre-incident assessment. However, if such information is not used properly, and in conjunction with other data, an organization may find significant losses related to its product designs, research and development (R&D) operations, competitive processes, patents, and other intellectual property.

For other enterprise-specific issues such as information technology (IT), the outsourcing to IT risk consultants can offer well-known approaches for understanding a firm's ability to fend off attacks. However, the expertise of those consultants often focuses primarily on risks within the IT structure – despite the fact that there are many other potential areas of risk that must be taken into account to fully protect a company's intellectual property.

For companies that rely on in-house personnel to meet their security needs, the basic problem remains the same. Although some organizations often prefer this solution – usually for fear of not wanting to reveal

vulnerabilities to outsiders – company personnel frequently focus their attention primarily on diagnostics, forensics, and basic security monitoring. Often, because of the nature of their employment, staff members: (a) may not be able to offer an objective assessment; and/or (b) do not necessarily possess a high enough level of expertise, and the investigative skills also required, to carry out a truly comprehensive analysis of the company as a whole.

Rather than focusing on security solutions in only one component of a firm's operations, a holistic intelligence program would diversify the collection of information across the entire enterprise. Use of this broader approach usually will help protect the intellectual assets of public- and private-sector organizations in the current age of sophisticated threats.

When pieces of a puzzle are missing, it is difficult to see the big picture. The same is true for detecting crimes related to information technology.

Holistic Security: A Deeper Look

Holistic security encompasses all of the functional units of a business enterprise: IT, human resources, legal, R&D, security, and many others. Such security is based on the premise that so-called "isolated incidents" occurring in one particular department should be juxtaposed with other data to: (a) corroborate the existence of possible vulnerabilities; and (b) help identify other negative trends. The following four examples demonstrate how various isolated incidents, when interpreted holistically, can help skilled investigators understand the nature of a possible threat directed against a company's key value drivers.

Isolated Incident No. 1. A member of a company's IT Department observes Employee A trying to gain access to a folder for which the employee does not have permission to access. This folder contains sensitive information on a prototype development not yet introduced to the market. A week later, the same employee was found running a scan of the company's internal network. When IT staff noticed this activity, they confronted the employee, who offered what the staff considered to be a plausible explanation. No subsequent action was taken; and the information was not shared with any other department within the company.

Isolated Incident No. 2. The office manager has noticed Employee A working late hours – an irregular and seemingly unnecessary activity. Late one evening, Employee A attempted to leave the building with a bag containing folders labeled "proprietary." When the office manager questioned the employee, the latter responded with a frantic apology and offered a plausible explanation. Accepting the response as legitimate, the office manager did not share this information with anyone else in the company.

Isolated Incident No. 3. A different employee (Employee B) recently traveled overseas to attend a meeting with a foreign partner on a joint venture opportunity. During the trip, the employee traveled with not only his smartphone but also a company laptop – both of which contained proprietary information. Moreover, on more than one occasion, Employee B had accessed the U.S. company's network from the joint venture partner's internal network. Apparently not thinking anything of it, Employee B did not, after his return, mention those actions to any of his colleagues.

Isolated Incident No. 4. At lunch on a Monday morning, colleagues learned that Employee A had just returned from a weekend trip overseas. When asked for details about the trip, the employee offered a hurried and somewhat confusing explanation about a "weekend getaway" that appeared to be in conflict with his/her established lifestyle pattern. Later that day, colleagues learned that Employee A had traveled with numerous company thumb-drives and disks – also rather unusual behavior for a traveler supposedly on a vacation. Moreover, over a longer period of time, colleagues started to notice some unexplained affluence on the part of Employee A – driving a brand new car, for example, rather than the more modest vehicle Employee A previously drove. When queried by a colleague, Employee A stated somewhat awkwardly that the car had been a gift from a distant relative. Without additional information confirming the suspicions already aroused, however, the issue was dropped; and the information already developed was not shared with anybody else inside the company.

Share, Study, Assess & Confirm

As individual data points, the preceding incidents may seem mundane and/or ordinary to those who witnessed the various actions mentioned. But if those incidents had been documented, and not only correlated but also analyzed with the information collected from the other departments, certain patterns might well have emerged that would confirm the incidents as potential evidence pointing to a targeted campaign to steal the company's intellectual property.

In an era of increasingly sophisticated threats, the protection of intellectual assets may best be served through adoption of a holistic approach to security using both trusted intelligence methodologies and properly trained personnel. To do anything less, in fact, could have disastrous consequences. The failure "to address the challenge of trade secret theft costs industry billions of dollars each year," said Pamela Passman, president and chief executive officer of CREATe.org, a leading nonprofit dedicated to helping companies, suppliers, and business partners reduce piracy, counterfeiting, and trade secret theft. Moreover, she added, such thefts "can have devastating reputational, financial, and legal impacts … [not only] for individual companies … [but also for] the global economy as a whole."

Armond Caglar is a security solutions consultant at Tailored Solutions and Consulting (TSC), an enterprise risk consultancy based in Washington, D.C. Prior to establishing himself in his current position, he served in the U.S. government for more than seven years conducting worldwide operations in support of sensitive national-level priorities. He holds both a Master's degree from Tufts University and a Bachelor of Arts degree from the University of New Hampshire.

Incident Gridlock – Overwhelming a City

By Glen Rudner, Transportation

Without warning the City of Boston was thrown into chaos on 15 April 2013. The terrorist bombings that occurred near the finish line of the Boston Marathon killed three people, injured dozens more, and gridlocked an already congested city. Because both manmade and natural disasters can happen anywhere at any time without warning, the transportation infrastructure is critical to emergency response. Regardless of whether transportation facilities are directly affected by the incident, transportation is a vital link needed to bring responders to the scene, transport the victims to medical facilities, and move the public away from potential harm.

Information, resources, as well as understood and effective procedures that are rehearsed with other emergency responders, are needed in order to achieve an efficient response across the transportation network. In and around large metropolitan areas or other locations where there are a lot of commuters, most people are already familiar with the effects of regular daily traffic congestion. What may not be realized is the effect that heavy congestion can have on the emergency response agencies. Such gridlock has a tremendous impact on the commuters' personal, business, and social lives, but has as much if not more of an effect on the ability of responders to navigate to the scene of an unexpected incident or even a planned event.

Bombings, Hurricanes & Other Past Disasters

When an incident occurs and a request for an emergency response is made, emergency vehicles will often take longer to reach their destination due to the amount of congestion that builds following an incident. The gridlock that ensues is part of a recipe that causes a delay in treatment or mitigation of the incident as well as additional problems with traffic movement. The Boston bombings caused a gridlock of epic proportions because, in addition to the incident itself, all modes of transportation into and out of the city were virtually shut down for nearly a day.

In light of the attacks of 9/11 and natural disasters such as Hurricanes Floyd (1999), Katrina (2005), and Rita (2005), the Federal Highway Administration conducted a study in 2007 to address several transportation issues that had emerged. The results showed that, after an incident occurs, there is:

- A weakness in the infrastructure's ability to handle the movement of people;
- Anything suspicious occurring near a transportation facility will cause the facility to either close or at least restrict access; and
- As found during the 2002 "D.C. Sniper" attacks that lasted more than 20 days – killing 10 people and injuring three more – traffic congestion increased as law enforcement investigations were conducted at entrance and exit ramps to major arteries.

Another issue that had surfaced was that few government agencies at the local, state, and federal levels integrate transportation into their emergency management plans. For example, according to the 2007 study:

- Less then 50 percent of all government agencies include details on media coordination, traveler information, and infrastructure protection;
- Only 10 percent address transportation coordination with local, state, and federal level emergency operations centers; and
- Only 66 percent of state and 33 percent of local plans have Department of Transportation contacts.

Another important aspect that has not been thoroughly addressed is that personnel who respond from the transportation sector may not be familiar with local and state emergency management procedures. Some have not been trained to work within the Incident Command System nor are they familiar with the National Incident Management System. There are states and local jurisdictions that have made great strides in filling this information gap, but much is still needed – in particular, preparing the transportation sector with both the equipment and training to deal with terrorist threats.

When transportation is disrupted because of a natural or manmade disaster, it not only hinders people from evacuating the affected area, but also delays responders from reaching those in need.

Planning & Technology Initiatives

The Federal Highway Administration is currently working with transportation agencies nationwide – along with their many partners – to improve coordination in the planning and technology processes. By integrating and improving regional and transportation operational plans to coordinate with current emergency operations and response plans, these plans will reflect not only how the transportation system will work, but how it will work during emergencies. However, it is important that transportation agencies and response organizations continue to build more effective working relationships – including multiagency, multimodal exercises that are conducted as tabletops and full functional exercises to build relationships and test the plans' functionality.

In addition to planning initiatives, the transportation sector has many advanced technological tools that could be used to assist emergency responders in expediting evacuations – from rerouting traffic to full-scale lane reversals. Although many transportation agencies have the tools already in place, they have not yet tested and integrated them with emergency response organizations. A common understanding of the Incident Command System and its use during incidents would ensure better management of an incident and efficient deployment of transportation assets. Fortunately, some of this training has already begun and is now becoming an integral part of the required training.

In summary, normal everyday traffic can cause disruption and confusion, but even more so during and

immediately following a disaster incident. The duration of the disruption and the effectiveness of the emergency responders and transportation system, though, will be determined by the plans in place, the training conducted prior to the incident, and the level of familiarization with designated roles and responsibilities. It is difficult to prepare for every eventuality, but if risks and hazards – those with the greatest likelihood and with the highest potential impact on operations – have been identified, emergency plans put in place, and effects minimized with mitigation procedures, personnel will be ready to respond with confidence. Through repetition of exercises, cross-discipline training, and application of standard operating procedures, cities will be better prepared to manage the gridlock that often follows both planned events and unplanned incidents.

Glen Rudner is an independent consultant and trainer who recently retired as a Hazardous Materials Response Officer for the Virginia Department of Emergency Management. His 35 years of experience in public safety includes 12 years as a career firefighter/hazardous materials specialist for the City of Alexandria (VA) Fire Department; he also served as a volunteer emergency medical technician, firefighter, and officer and, as a subcontractor, served as a consultant and assisted in the development of many training programs for agencies such as the Federal Bureau of Investigation, the International Counter-proliferation Program, the U.S. Department of Justice's Office of Justice Programs, the U.S. Department of Homeland Security, and the Defense Threat Reduction Agency. He is now Secretary for the National Fire Protection Association Hazardous Materials Committee, a member of the International Association of Fire Chiefs' Hazardous Materials Committee, a member of the American Society of Testing and Materials, and Co-Chairman of the Ethanol Emergency Response Coalition.

The Island Life – Isolated But Not Alone

By Joseph Cahill, EMS

New Shoreham, which encompasses Block Island located off the Atlantic coast of Rhode Island, is home to 1,010 year-round residents, according to the 2010 U.S. Census, and covers a total geographic area of slightly less than 10 square miles. The Block Island Volunteer Fire and Rescue Department (BI-VFD) provides fire and emergency medical services (EMS) for the entire island community.

Despite the limited number of full-time residents, the island hosts numerous special events each year ranging from those – a Fourth of July fireworks celebration, for example – celebrated in hundreds of other towns and cities across the United States as well as several others, such as a week-long sailboat race unique to Block Island itself. In several ways, though, the most significant special event for BI-VFD itself is preparing each year for the additional 15,000-20,000 summer vacationers, many of them from overseas, visiting the island on almost any given day during the summer.

Self-Sufficiency & A Solar-Powered Ambulance Barn

Geographic isolation is an ever-present factor that obviously must be considered in any and all emergency responses on Block Island because many traditional sources of help – provided through mutual-aid agreements from neighboring towns just a few miles up the road – are simply not available. The island's solution, therefore, is an uncommon degree of self-sufficiency, which means: (a) making do with what is already available on the island 24/7; (b) always looking for, finding, and using better ways to meet most foreseeable emergencies; and (c) finding nontraditional as well as traditional partners to help as and when needed.

In 2007, when the BI-VFD's ambulance barn was being replaced, the cost was borne in part by the Town of New Shoreham itself through a fundraising drive within the community, supplemented by grants and various donations in kind from local businesses. Thanks in large part to that local support, the facility was built *by* the community, *for* the community.

Unknown Chemical or BioHazard?

AP4C Handheld Chemical Detector

Known Solutions

AP4C-F Fixed Location Chemical Detector

- Unlimited, Simultaneous Detection
- Fast and Easy to Use
- Always Ready with Very Low Operation Cost
- Rugged Construction for Harsh Environments

PROENGIN

Chemical and Biological Detection System

PROENGIN, inc. | 140 S. University Dr, Suite F, | Plantation, FL 33324 USA
Ph: 954.760.9990 | contactusa@proengin.com | www.proenginusa.com

Two closely related challenges addressed at the same time the new construction was proceeding were ensuring that: (a) sufficient supplies of portable oxygen would be available in the future; and (b) there would be a reliable source of emergency power available when needed. It was determined that the best way to meet the first challenge was to find a reliable way to refill the portable oxygen cylinders that would be stored in the new ambulance barn. The previous system, which required the constant replacement of empty cylinders with filled ones ferried in from the mainland, therefore was replaced with a system that concentrates the oxygen on-site – similar to an oxygen-concentration system designed for use by individual patients who require a continuing supply of oxygen in their own homes.

Thanks to a working partnership with the Block Island Medical Center, the new system installed in the ambulance barn now supplies all of the oxygen needed by both the Medical Center and the BI-VFD itself. The same approach was used in resolving the need for a reliable source of emergency power. More specifically, the ambulance barn was designed to meet its own continuing needs with an array of solar power charged batteries – enough, in fact, to power the barn for up to six days.

Sharing Ideas, Self-Reliance & Building Mutual Aid

Many of the island's other emergency solutions are similar to those used on the mainland – for example, dispersing emergency resources in various convenient locations throughout the island to ensure availability. As in various other U.S. jurisdictions, a Semi-Automatic External Defibrillator program also has been implemented to install life-saving devices not only in most fire and police vehicles but also in a number of the island's public buildings and hotels – thereby significantly improving the survival chances for cardiac arrest patients.

According to BI-VFD's Fire Chief Tristan Payne, mutual aid agreements also have been completed with a number of mainland fire departments, but it is recognized that the travel distances involved pose additional challenges for response times. When responding to an emergency situation, firefighters outfitted with hand tools and bunker gear could arrive by air within 12-15 minutes or so, but any fire apparatus and/or other necessary resources may take up to several hours by ferry – weather permitting.

When coping with a mass-casualty incident, the BI-VFD has a trailer that is already stocked with medical supplies and readily available for any incident creating a large number of patients. If additional services and/or resources were needed from the mainland, the Rhode Island-1 Disaster Medical Assistance Team (DMAT) would be deployed to the island to provide an emergency hospital and other medical resources.

During Hurricane Sandy in 2012, the local flooding was significant enough that the main rescue barn became part of an island within the island. To maintain service throughout the community, one ambulance was stationed at the barn while others were deployed to various locations on the island. Privately owned 4x4 trucks were then used to move EMS personnel and their equipment to the locations in greatest need at any given time, a process that helped maintain coverage for the entire island despite the main base being isolated by the storm.

In summary, the BI-VFD has had to adapt to a unique and somewhat uncompromising geography, but so do many other communities. Those on other islands, and/or on the mainland itself, can easily borrow a page from Block Island's emergency playbook to upgrade and strengthen the safety of their own populations – and visiting guests. By effectively communicating with, and forming strong ties to, outside resources, communities can maximize the combined effect of all available emergency resources. As Bryan Wilson, BI-VFD's EMS Captain, sums it up, "Out here, we take care of each other."

Joseph Cahill is a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as citywide advanced life support (ALS) coordinator for the FDNY – Bureau of EMS. Prior to that, he was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. He also served on the faculty of the Westchester County Community College's Paramedic Program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.

A Major Step Forward: Private Sector Resilience Coordination

By Joseph Trindal, Private Sector

Over the past two decades, the public sector has started to recognize the private sector as a key partner in emergency preparedness, response, and recovery operations. Moreover, as local, state, and federal agencies have refined their own efforts to prepare for, respond to, and recover from major natural disasters, the role of the private sector as a co-partner not only has become more prominent but also has made that sector much more than a consumer of emergency management services. Today, in fact, the private sector's broad array of services, goods, and supply-chain interdependencies is vital for maximizing response efficiencies and achieving the timeliness needed in responding to any major disaster.

The whole-of-community response to Superstorm Sandy in 2012 set the stage for redefining "community" on a truly national scale and now recognizes the private sector as not only consumers of emergency services but also as the delivery partners needed to distribute and disseminate those services. Even before Sandy, however, many communities throughout the country had already: (a) recognized the urgent need for major improvements in preparedness; and (b) started developing the capacity needed for assessing, coordinating, and managing the broad range of private sector capabilities needed to expand and improve all-hazards response and recovery capabilities. To help address these and other diverse needs, there also has been increased interest in and support for the creation and staffing of business-oriented Emergency Operations Centers (EOCs).

There is greater value in this approach than there was in simply leveraging private sector input or representation at an existing public sector EOC when a disaster occurs. Business EOCs have continued to be refined since their inception in the mid-2000s. The Federal Emergency Management Agency (FEMA) leads the new and much more collaborative effort – in large part through the BEOC Alliance, a consortium of private businesses, nongovernmental organizations, academia, the U.S. Department of Defense, and many other partners.

In the very near future, according to current plans, the District of Columbia (D.C.) will formally announce the opening of the D.C. government's own Business Emergency Management Operations Center (BEMOC). The D.C. BEMOC will be extremely well positioned as a standing entity within the District's own Homeland Security and Emergency Management Agency. Although D.C. itself is not a particularly strong commercial or industrial national asset, it nonetheless possesses several unique advantages and opportunities for emergency managers at all levels of government. Moreover, because the District is a jurisdictionally compressed area, the city's officials recognize the need to leverage all local assets in a coordinated and integrated manner in order to manage and cope with the full spectrum of potentially disruptive risks.

The Mirroring of Selected Emergency Support Functions

The D.C. Homeland Security and Emergency Management Agency's BEMOC is aligned with six key sector areas described in the 2013 Presidential Policy Directive 21 – better known as the Critical Infrastructure Security and Resilience Directive – and will undoubtedly be included in upcoming revisions to the National Infrastructure Preparedness Plan. The key BEMOC sectors, which also mirror applicable components of the city's and nation's emergency support functions, are (not necessarily in this order of importance): Food, Financial Services, Fuel, Transportation, Hospitality, and Medical.

Inclusion of the private sector, as structured at the BEMOC, is expected to achieve not only greater depth in sector-specific capabilities but also to expand the breadth of sector interdependency preparedness and management responsibilities. The BEMOC structure and functionality have not only incorporated the "best practice" examples of other business EOCs – in, such states as Rhode Island, Missouri, and Louisiana, as well as FEMA's National Business EOC – but also have revised and tailored those examples to better serve the District's unique and nationally prominent environment.

BEMOC Operations & Future Role

The BEMOC will operate, according to current plans, as both a brick-and-mortar facility and a virtual entity. Representatives from each of the sectors mentioned above will

be selected by the BEMOC leadership and will be expected to quickly respond to the BEMOC after activation of any major incident or event. The virtual interaction planned is expected to bring additional depth to each sector through a broad array of interactive communication options. Moreover, because of and thanks to the sector-specific preparedness liaisons developed, coupled with duplicative communications capabilities, the BEMOC as a whole will be uniquely scalable in operations ranging from routine events to extreme incidents.

As a standing element within the Homeland Security and Emergency Management Agency, the BEMOC will serve primarily in support of public sector emergency management initiatives. However, the BEMOC's role in mapping and cataloging private sector capabilities and assets in advance of an event is expected to greatly improve efficiencies in public sector responses. In addition, BEMOC's direct private sector connectivity will speed the uniform dissemination of messages, enhance overall community-based situational awareness, and even help guide future decisions on resource allocation. BEMOC's intricate private sector network also should be of significant value during post-disaster recovery operations.

In the preparedness field per se, the BEMOC will play a significant role in establishing uniformity with and cohesion to and throughout the current widely disparate array of private sector preparedness plans. A fundamental BEMOC goal is to be as inclusive as possible of sector-specific business interests so that opportunities for training, information sharing, exercises, and other preparedness activities will be much more widely available – thereby enhancing community resilience as a whole. To help meet that goal, BEMOC is already engaged with various community groups, including: the D.C. Hospitality Association, the D.C. Hispanic Chamber of Commerce, the InfraGard National Capital Region Members Alliance, and many others.

Participation Values – Plus a Long Look Ahead

Private business participation in BEMOC offers a number of rewards that are good for business as well. Participation is free and highly adaptable to the capacities and desires of individual businesses. Participating companies must have a physical presence within D.C., of course, but it is expected that the BEMOC concept will become more inclusive and expand throughout the entire National Capital Region.

Whatever happens in the future, though, it seems clear that, by establishing a formal relationship with BEMOC, local businesses will receive more sector-specific and locality-specific messages than are currently available through the Homeland Security and Emergency Management Agency.

Members also will have access to the Center's business-to-business portal, an invaluable tool for information sharing and the development of immediate and more accurate situational awareness. BEMOC participants also will receive timely notices of upcoming briefings, training exercises, and best-practice programs. Of perhaps even greater importance, BEMOC participants will network on a continuing basis with other key personnel within each participant's interdependency matrix, as well as with public sector emergency services providers, to develop and strengthen overall community resilience. Whatever else happens, it is reasonably anticipated that business values and returns on investment may, in extreme cases, determine whether the business even exists after the disaster.

In short, the business EOC practice is expanding throughout the United States. The D.C. government's adoption and support of the BEMOC serves as just one important example of what seems to be a rapidly growing national trend. Moreover, as public sector budgets decrease, greater community-based integration with the private sector will become even more essential.

However, effective integration in delivering sustained resilience cannot in any case be limited to the occurrence of a disaster event or incident. Effective whole-of-community resilience requires significant and sustained advance work – for which it is difficult to quantify profitability and/or return on investment. Nonetheless, the still relatively new business EOC model is and will continue to serve as a best practice for business profitability as well as public sector service quality in fiscally austere times.

Joseph Trindal is president and founder of Direct Action Resilience LLC, where he leads the company's portfolio of public and private sector preparedness and response consulting, training, and exercise services. He also serves as president of the InfraGard National Capital Region Members Alliance. He retired in 2008 from the U.S. Department of Homeland Security, where he had served as director for the National Capital Region, Federal Protective Service, Immigration and Customs Enforcement. In that post, he was responsible for the physical security, law enforcement operations, emergency preparedness, and criminal investigations of almost 800 federal facilities throughout the District of Columbia, Northern Virginia, and suburban Maryland. He previously served, for 20 years, with the U.S. Marshals Service, attaining the position of chief deputy U.S. marshal and incident commander of an emergency response team. A veteran of the U.S. Marine Corps, he holds degrees in both police science and criminal justice.

Seeing National Preparedness Through the Public Health Lens

By Raphael M. Barishansky, Public Health

As is required by the Presidential Policy Directive 8 – better known as the 2011 "National Preparedness" Directive – the Federal Emergency Management Agency (FEMA) is required to develop and release an annual National Preparedness Report (NPR). That report summarizes the areas not only where the nation has made significant progress but also where there are still major challenges that must be faced – particularly with regard to the various elements of preparedness outlined in the 31 core capabilities postulated in the National Preparedness Goal.

The first NPR, issued in 2012, showed that there has been significant progress in the preparedness and response capabilities that the United States has focused on since the 9/11 terrorist attacks. The 2013 NPR, released in May, focuses primarily on the preparedness and response accomplishments either achieved or reported during 2012. It also: (a) reviews the nation's overall progress in strengthening national preparedness; and (b) identifies several areas where preparedness gaps remain.

The overall state of public health and its various preparedness components were discussed at length in the 2012 NPR. Among the specific initiatives and areas highlighted were the nation's biosurveillance capabilities, the progress achieved in surge planning, the federal coordination of medical countermeasure efforts, and – last but certainly not least – current and future funding realities. The 2013 NPR touches on many of the same areas of public health preparedness, and highlights both the additional progress made and the numerous challenges remaining.

Successes: Closer Coordination, Biowatch & Fatality Management

The "Overarching Findings" section of the 2013 NPR spells out one of the more interesting findings specific to public health: "Whole community partners continue to use preparedness assistance programs to maintain capability strengths and address identified gaps, while key federal sponsors are identifying strategies to improve program effectiveness and efficiency." The same section outlines the improved collaborative effort between grantors – specifically, the Office of the Assistant Secretary of Preparedness and Response within the U.S. Department of Health and Human Services (HHS) and the Centers for Disease Control and Prevention (CDC) – to better define essential public health and healthcare preparedness capabilities.

That effort led to Hospital Preparedness Program applicants and Public Health Emergency Preparedness applicants having the ability, since May 2012, to submit a single application for both cooperative agreements at the same time. This improved program alignment not only fosters closer coordination among public health and healthcare system partners at all levels of government but also improves efficiency in grant administration.

Among the other key findings specific to public health in the report are the following:

- The national biosurveillance system, also known as Biowatch, is a system designed to identify releases of aerosolized biological threat agents – specifically including anthrax, tularemia, and other pathogens. The Biowatch system, already in place in more than 30 large metropolitan areas, relies heavily on collaboration between federal, state, and local partners. One of the most important successes of the program, as noted in the 2013 NPR, is the 15-hour operational response time achieved to answer biosurveillance queries – less than one-third of the performance target of 48 hours. That remarkable achievement translates directly into a more rapid notification of the possibility of a biological release – and, therefore, significantly more time to respond.

- The 2012 NPR noted that the overall number of states with state-level fatality management plans had increased from 64 percent to 96 percent. However, some of those plans were not yet adequate or fully actionable, so there was still a potential reliance on the use of federal assets to cope with certain incidents. The 2013 NPR shows that additional progress in this area was made in 2012, specifically including the fact that HHS had finalized its own fatality management concept of operations (which involves, among other

things, the management of mass fatalities in disasters that result in fewer than 5,000 fatalities). HHS took another step forward by hiring its first national program coordinator for fatality management. These accomplishments, combined with the inclusion of fatality management in the CDC's own public health preparedness capabilities, focus additional and much needed attention on fatality management.

- One of the operationally based successes described in the 2013 NPR outlines the public health response elements specific to Hurricane Sandy, including the speed at which assets were moved to the affected areas. Traditionally, HHS has postulated a 24- to 48-hour time frame for deploying National Disaster Medical System (NDMS) resources – personnel and equipment, primarily – following a major incident. However, in the case of Sandy, the report stated that two NDMS Disaster Medical Assistant Teams arrived onsite in New York within four hours, well ahead of the time frame usually projected.

Nursing Home Challenges

The report is not all positive, though – and also highlights certain areas that require improvement or could prove to be an issue in the future. One such area involves the emergency readiness of nursing homes, and is described as follows: "While a large majority of nursing homes met federal emergency planning and preparedness requirements in 2011, experiences during recent disasters indicate that many nursing homes may not be as prepared as these figures suggest."

In the past, nursing homes have not been as much of a focus as they have been during recent events. Some unique challenges that nursing homes face in developing realistic and actionable emergency plans include the ability to: carry out facility evacuations, establish pre-incident communications with other emergency partners, and complete pre-established transportation contracts for residents. There have been some incidents in which it was difficult to track residents who had been evacuated to other nursing facilities. Following Sandy, various nursing homes reported experiencing some of the aforementioned issues as well as other concerns related to family notifications and ensuring the availability of adequate food and medical supplies.

Funding Realities & Future Problems

There is an important cautionary tale in the report as well – one that is specific to the reality of how reductions in public health funding and personnel could affect the progress already achieved. Here it is important to remember that most state and local public health agencies pay for their public health preparedness efforts primarily with federal funds. As such, cuts to these funding streams, combined with the job actions that may result from furloughs or layoffs, could substantially impact the progress that will be reported in the 2014 NPR.

Several major organizations – for example, the Association of State and Territorial Health Officials, the National Association of City and County Health Officials, and the Trust for America's Health – have repeatedly made it clear that the job cuts that state and local public health agencies already have experienced will have an adverse impact on the nation's overall public health preparedness realities. This impact will no doubt lead to some difficult consequences in future real-life incidents where public health plays a critical role in disease surveillance and detection, the mass prophylaxis of populations with antivirals, pandemic response, and other areas.

Nonetheless, public health agencies across the United States still stand at the ready to play a significant role in preparedness and response to all types of emergencies. Daily threats, whether a naturally occurring event – for example, H7N9 and the still evolving Middle East Respiratory Syndrome – and/or manmade incidents, continue to make headlines and highlight the need for a robust, well-prepared, and highly capable public health work force.

The latest NPR shows that, although local and state health departments are now better prepared for emergencies than ever before in the nation's history, there is now an ever-present concern that the funding cutbacks seen in the various public health preparedness grants will adversely impact the agencies that sit at the tip of the spear in protecting the American people during future public health emergencies.

Raphael M. Barishansky, MPH, is the director of the Office of Emergency Medical Services (EMS) for the Connecticut Department of Public Health. Prior to establishing himself in this position, he served as chief of public health emergency preparedness for the Prince George's County (Maryland) Department of Health and as executive director of the Hudson Valley Regional EMS Council, based in Newburgh, N.Y. A frequent contributor to the DomPrep Journal and other publications, he can be reached at rbarishansky@gmail.com.

Subject Matter Experts & the Theory of Relativity

By Sheri Donahue, Private Sector

The term "subject matter expert" (SME) started as a quick and easy description of anyone with specialized knowledge who worked with software developers. Such persons might not possess specialized expertise in information technology itself, but would be much more knowledgeable than the average person in the many fields in which the software will be used. Over time, the SME term has evolved to mean anyone with special expertise in a particular topic. In many instances, the person designated an "SME" might not even consider himself or herself to be a true "expert," as that term is generally understood. However, he or she does know more about the relevant subject area than others who are responsible for gathering and collating the information needed for a specific project. So the SMEs are in fact experts, relatively speaking.

Another term that has become all too familiar is "reinventing the wheel." If the leader of a project, a federal agent, or a manager is working on a project, case, or program involving an area in which he or she has either no or only limited knowledge, the information he or she needs usually is available on the internet. However, locating that data may well take a considerable amount of time and require pulling together bits and pieces of information to create the "big picture" needed for the context of the specific project or case on which the non-expert is working. In most cases, simply being able to talk with someone whose background is in the same field can save considerable time and a great deal of effort. What this means, in essence, is that it is almost always easier to find the "wheel" than to build one from scratch – and perhaps risk leaving out one or more important aspects of the topic.

InfraGard – The Early Years

In 1996, the Federal Bureau of Investigation (FBI) was working on a case in Cleveland, Ohio, that involved the then fairly young field of information technology (cyber). At that time, the FBI Cyber Division was not yet in existence. However, as the designated federal domestic law enforcement agency, the FBI has always been the federal agency assigned the responsibility for investigating many types of crimes. In the not-so-distant past, of course, cyber was not well understood as a developing technology – nor were the many ways in which it could be used for criminal purposes. Therefore, the agents working the cyber case in Cleveland met with private sector SMEs in information technology in order to further their case.

InfraGard provides an important link between law enforcement agencies and subject matter experts. By working together, the public and private sectors are better equipped to solve a variety of criminal cases.

These relationships helped the FBI significantly and led to the creation of a new professional organization, InfraGard, which over the next few years quickly expanded to all FBI field offices across the country. Individual chapters were established and the organization's membership grew rapidly. Although the principal focus of InfraGard in the early days was primarily on cyber security itself, the organization has expanded its fields of interest over the years to include all infrastructure sectors.

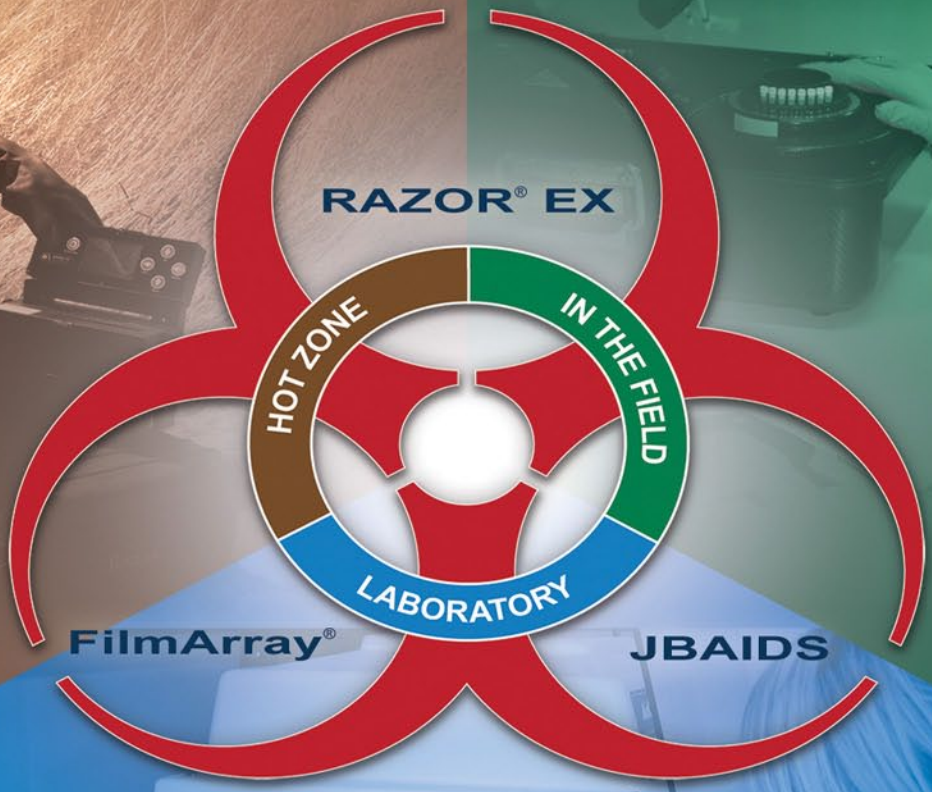
That rapid expansion may have been the result of two driving factors: (a) cyber security has become a major concern within all sectors of the nation's public and private sectors alike; and, (b) the public-private partnership model in which the private sector is a key player in matters of national security has proved to be very successful. Today, the organization's membership consists largely of the owners and operators of the critical infrastructure – including, of course, the SMEs working in their various sectors. More formally, InfraGard is known today as a public-private partnership between the FBI and the private sector owners and operators of the nation's critical infrastructure.

As InfraGard grew to include thousands of members across the country in many different sectors, it became obvious that the organization would experience

BioSurveillance

Flexible, Accurate, Proven Ready

BioFire Diagnostics delivers a fully integrated suite of Biological Agent Identification Systems. Since 1998 we have fielded BioSurveillance products that span the range of operations from the lab to the field, clinical diagnostics to environmental surveillance.



Idaho Technology is now

BIOFIRE DIAGNOSTICS, INC.

Discover the system for your mission.

WWW.BIO-SURVEILLANCE.COM

either: (a) a major challenge (to ensure that local chapters served the disparate interests of the members); or (b) a welcome opportunity to develop a formal structure in which its members could both gain additional expertise and contribute more effectively. Taking it as an opportunity, the organization itself could become more effective as well.

Sector Chiefs – Organizing & Connecting

Some of the InfraGard chapters recognized this opportunity quickly and created various ways to organize their membership in a logical manner. One result was the "Sector Chief" initiative, which was created in the Kentucky chapter in 2003. In simplest terms, this initiative involves organizing the membership by critical infrastructure sector and appointing a sector chief for each to represent them. For the Kentucky chapter, that requirement resulted in an increase in membership, greater participation in meetings, an improved integration with local organizations, and even the development and execution of sector-specific tabletop exercises. The methodology used by the Kentucky chapter was shared in 2004 with other chapters – some of which already had similar structures in place. Other chapters used the Kentucky model to establish their own Sector Chief programs.

Over the past several years, InfraGard has continued to grow and the FBI has recognized the benefits realized by chapters that have a Sector Chief program in place. Therefore, the program that started as a private sector initiative will soon be implemented by all chapters with the support of the FBI coordinators assigned to each chapter.

As the Sector Chief model expands, it also seems inevitable that there eventually will be regional sector chiefs connecting chapters across the nation. If and when this happens, those in a specific sector in the southeast region of the United States, for example, will have a quick and effective way to connect and communicate with other InfraGard members in the northwest and other regions. This new capability will not only help those seeking an SME to provide the missing context needed for a specific project or individual case, it also will benefit all InfraGard members who have a need to collaborate with other InfraGard members anywhere in the country.

External Benefits of Partnerships

Additional benefits also have been realized by organizations outside of the FBI. The U.S. Department of Homeland Security, to cite but one example, provides Protective Security Advisors (PSAs) across the country with a mission to assist in expanding and improving the protection of critical infrastructure. The DHS PSAs become members of InfraGard and have direct interaction with the other InfraGard members. Therefore, they are able to connect more easily with the SMEs without having to reinvent the wheel.

In addition to the obvious benefits provided to the FBI and DHS, there are many ways in which the nation's other public and private sector agencies – state fusion centers and governors' offices, for example – can be helped by various InfraGard chapters. Perhaps of greatest importance, though, is that InfraGard continues to benefit its own members by, among other things, giving them immediate access to other SMEs, additional training opportunities, and informational documents on sector-specific threats/vulnerabilities. In these and many other ways, InfraGard members will have the continuing opportunity to contribute to their local, state, and national security in meaningful ways that only they, as the subject matter experts, can.

Sheri Donahue is program manager for security and intelligence at the Indian Head Division of the Naval Surface Warfare Center. She previously served: as director of customer support for DisastersNet Inc.; as managing director of the InfraGard National Members Alliance (INMA); and as executive director and president of the Cyber Conflict Studies Association (CCSA) at the Norwich University Applied Research Institutes. She also served, for 16 years, as an engineer and special programs manager for the Department of the Navy. She has been with InfraGard since 2003, served on the National Board from 2004-2012, and is currently the national president.

Hackers & Federal Agencies: Broken Connections

By Rodrigo (Roddy) Moscoso, Viewpoint

Over the past 20 years, the annual so-called "hacker" conference (DEF CON), has served as a welcome and much needed opportunity for collaboration among computer hackers. Attendees have included government agents, commercial industry professionals, and private citizens seeking to learn more about the tradecraft of cyber security – including the latest technologies and methodologies used for legal (and perhaps less than legal) data access.

For its 1-4 August 2013 conference in Las Vegas, Nevada, the organization's "call for papers" noted that a special focus would be on "new ways to approach security and privacy, as well as building a community that is open to new ideas. Everything from the most complex modern technology to hacking grandma's toaster through Bluetooth is fair game," the announcement continued. "Show us and the world what you have been up to and what attack exploits, defensive techniques, or unique research you have been working on."

If members of the nation's hacker community cool to the idea of sharing their intelligence and experience in cyber security with the federal government, the losses may be both costly and long-term.

A Strained Relationship vs. "The Greatest Demand"

Presenters from previous years included National Security Agency (NSA) chief General Keith Alexander, USA (Ret.), who delivered the 2012 DEF CON keynote speech and, in it, directly solicited the assistance of the hacker community to improve U.S. cyber security operations so that, "We can protect privacy and civil liberties as we improve security." He also noted that the expertise of DEF CON attendees is now – and for the foreseeable future, he implied – "in the greatest demand for our nation."

However, following the recent public revelations of Edward Snowden – the system administrator who leaked top-secret information to the press about U.S. and British surveillance programs, including the NSA's own "PRISM" surveillance and information-gathering program – the "trust relationship" between the government and nongovernment sectors has become strained. So much so, in fact, that DEF CON founder Jeffrey Moss asked federal representatives not to attend the conference this year.

The impact of this "unvite" could have significant implications for the federal government's ability: (a) to learn more about the latest trends in cyber security; (b) to attract the cyber industry's "best and brightest" to government service; and (c) to continue to improve homeland security and, by doing so, further protect the nation's political, military, and economic interests.

In 2012, the NSA manned its own recruitment table on the vendor floor at DEF CON. The agency's unusual public presence was not a major surprise, though. With an annual attendance at DEF CON of 8,000-10,000 security experts, the NSA and the other so-called "three-letter" government agencies usually represented find themselves in a truly unique recruitment environment – one in which there are literally thousands of highly skilled hackers in the same place at the same time. At least some of them may find the idea of helping the federal government protect itself against local and international threats to be not only personally and politically appealing but also professionally rewarding.

A Perceived Betrayal & The Chinese Challenge

On the international front, it is well known that other nations, notably China, are relentlessly working to hack into both U.S. government and commercial sites for both strategic and economic gain. Recognizing the proficiency of the Chinese hackers, DEF CON attendees might find it the ultimate challenge to help protect U.S. interests from the best hackers in China.

Unfortunately, there will be no formal government recruitment at DEF CON 2013 – at least partly because of the perceived betrayal among some members of the hacker community who believe that the Snowden revelations violated the unwritten trust agreement between the U.S. government and the nation's hacker communities.

Of course, DEF CON is not the only hacker conference available for government attendance (formal or clandestine), but it has clearly become one of the most collegial. In previous years, in fact, DEF CON hosted an entertaining "spot the fed" competition – in recognition of the fact that not every government employee at the conference was participating under his or her true credentials. However, the "spotting" game has become increasingly irrelevant in recent years as national security agencies recognized that it was better, and more productive, to be open about their true professional status. Perhaps the most important result of this new openness is that government professionals have been welcomed, and sometimes even sought out, at the DEF CON meetings by their counterparts in the hacker community.

Today, the trust factor has become relevant again, and the impact of the new and somewhat cooler relationship could go well beyond recruitment, in which case the end result could be significant economic losses as well as additional jeopardy for U.S. national security interests.

Billions of Reasons to Work Together

On 22 July 2013, the Center for Strategic and International Studies released a stunning report, underwritten by Intel/McAfee, that estimates the economic losses associated with cyber crime and cyber espionage to be many billions of dollars annually. The potential losses could be significant, because of: (a) the direct loss of intellectual property and research to sensitive strategic business information; (b) stock market manipulation; and (c) the costs of networking infrastructure and human resources charged with improving cyber security.

Although the original (2009) Intel/McAfee estimate that was cited by President Barack Obama of up to a trillion dollars lost to cyber crime every year was later found to be exaggerated, the revised (2013) figures – "billions, and perhaps hundreds of billions" – are nonetheless impressive.

In addition, on 23 July 2013, the Cloud Security Alliance released the results of a survey designed to assess the potential impacts of the disclosure of the U.S. PRISM program on the international cloud services community. Gartner estimates the global cloud services market to be $131 billion in 2013, an increase of more than 18 percent during 2012. Of the 500 survey respondents, 56 percent of non-U.S. residents indicated that they were less likely to do business with U.S.-based

cloud providers due to the Snowden revelations on PRISM. This could result in another significant impact to the nation's economy, which has historically led the international cloud services market.

This leads back to the need for the federal government to take a leadership role in engaging, rather than alienating, the private-sector hacker community. Unfortunately, the revelations related to the NSA's PRISM program may have squandered the good will established post-9/11. Today, the nation's "best and the brightest" in cyber might find their work in other industries. The most obvious and most immediate result would be that economic losses would continue to mount. More important, though, would be the obvious fact that the lack of in-house expertise might further dilute the effectiveness of the government's future cyber security operations.

NSA Chief Alexander is continuing his attempts to repair the damage caused by the Snowden disclosures – primarily through a media blitz aimed at both the Congress and the general public (and, presumably, the hacker community). He not only has emphatically defended PRISM, but also asserted during a session at the 2013 Aspen Institute Security Forum in Aspen, Colorado, that the U.S. government does not "have the technical capabilities" [to listen to everyone's phone calls or read their emails]. At the same time, he added that the disclosure of the PRISM operations to potential enemies of the United States has already caused "significant and irreversible damage to our nation." Assuming that those statements are accurate, recruiting the significant talents of current and future DEF CON attendees will be of critical importance in protecting the security of U.S. national interests – both human and economic – not only today, but also far into the future.

Rodrigo (Roddy) Moscoso currently serves as executive director of the Capital Wireless Information Net (CapWIN) Program at the University of Maryland, which provides software and mission-critical data access services to first responders in and across dozens of jurisdictions, disciplines, and levels of government. Formerly with IBM Business Consulting Services, he has more than 20 years of experience supporting large-scale IT implementation projects, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.