THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 9 NUMBER 8
AND HOMELAND SECURITY

FEBRUARY 2011
RESILIENCE

Contact: dhardy1@gmu.edu
703.993.8591

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

In this month's issue of *The CIP Report*, we focus on resilience. In particular, we highlight the link between critical infrastructure protection and resilience as well as the efforts of domestic and international organizations to enhance resilience.

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

First, the Vice President of Infrastructure Protection and Resilience at ICF International provides an overview of resilience and its significance to individuals, private organizations, and government agencies. Then, representatives from the Infrastructure Assurance Center at the Argonne National Laboratory, in partnership with the U.S. Department of Homeland Security (DHS), describe the formulation of a resilience index (RI). An Assistant Director at the U.S. Government Accountability Office (GAO), responsible for critical infrastructure protection issues with the Homeland Security and Justice Team, discusses two recent reports that analyze efforts by DHS to incorporate resilience into critical infrastructure planning and operations. The international perspective is conveyed by a Visiting Fellow of the Australian Defence Force Academy at the University of New South Wales, Canberra. Next, the Director of Risk Management, Supply Chain Development at the Coca Cola Company explores resilience as it relates to risk management. Finally, the last article reveals the need to include critical infrastructure resilience capacity in United Nations (UN) counter-terrorism assessments.

This month's *Legal Insights* examines the role of volunteer health care providers (VHPs) during a public health emergency.

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

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

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

What is Resilience?

by Lisa M. Bendixen, Vice President, Infrastructure Protection & Resilience, ICF International

Many individuals, organizations, and government agencies are struggling to define resilience. They wrestle with questions about what resilience is and what it is not; how it relates to protection, preparedness, and other existing concepts and initiatives; who should be responsible for overseeing or enforcing resilience; and how it should be measured. The very nature of how we address key problems and issues in our society today drives a need to define boundaries, assign roles and responsibilities, and keep score.

That approach sells resilience short. The ideal state for resilience is to embrace it as a way of life — to make it a part of our culture. One of Merriam-Webster's definitions for culture is, "the set of shared attitudes, values, goals, and practices that characterizes an institution or organization." Interpreted as a culture, many different approaches to managing risks can be a part of resilience — and that is a good thing. In fact, it is a very good thing as it lets us build on all the work that has been done to date to improve our resilience more quickly.

Resilience in its broadest sense is not new, but we have largely approached it in isolation, through approaches tailored to our own environment and responsibilities. Individuals and public and private organizations have developed contingency plans, continuity of operations plans, continuity of government plans, business continuity plans, disaster recovery plans, and emergency management plans and procedures. They have built or designed in redundancy, developed inventories of spare parts, trained back-ups, and set up alternate work sites. We do not want to throw out all these efforts; rather we want to build on and leverage them for greater effect. In some cases, this involves sharing best practices and lessons learned with organizations just starting their efforts. In other cases, it may mean thinking more broadly and optimizing at a higher level. This could be several companies working together or several communities/governments sharing technology and resources. Not only can a collaborative effort improve outcomes, it may drive costs down for any one participant in the collaboration.

A broad view of resilience allows many different groups to drive us forward and to work together. Individuals, governments at all levels, small business owners, large corporations, and even entire industries or sectors can all pursue a mix of separate and joint activities to preserve their operations and our

(Continued on Page 16)

Case in Point: Critical Infrastructure Protection and Resilience

There is much discussion about critical infrastructure protection versus resilience, yet these two concepts are inextricably linked and both are essential to our overall efforts to manage the risks to critical infrastructure. Drawing hard distinctions and separating protection and resilience can introduce vulnerabilities or lost opportunities at the margin if different parts of an organization are given responsibilities for the various approaches and fail to work closely together. Those in charge of protection might focus on screening goods and people entering facilities, while those in charge of resilience might want to ensure that the operations within the facilities are resilient through alternate work locations, telecommuting procedures, IT systems, etc. Either resilience or protection efforts could suggest redundant electric and water feeds to the operations — but if resilience and protection are considered separately, the cost-benefit analysis of these redundant feeds might underestimate the overall benefits.

An Index to Analyze Resilience of Critical Infrastructure

by Dr. Frédéric Petit, Michael Collins, and Ron Fisher, Infrastructure Assurance Center, Argonne National Laboratory

The world faces numerous threats from both natural and anthropogenic sources. In the first decade of the 21st century, in this Nation alone, we experienced several devastating events. Incidents such as the attacks on the World Trade Center in 2001, the Northeast blackout in 2003, and Hurricane Katrina in 2005 have had far-reaching impacts that have directly affected our society's well being. Although current efforts that have focused on preventing or mitigating the impact of future incidents have achieved admirable results, a more holistic approach is needed to improve the Nation's overall resilience. An all-hazards methodology that emphasizes not only preparedness but also robust response and recovery programs and capabilities is desired. The U.S. Department of Homeland Security (DHS) has defined 18 critical infrastructure and key resources (CIKR) Sectors that are essential to the Nation's security, public health and safety, economic vitality, and general quality of life.[1] If the operation of these CIKR Sectors is critical, their resilience must be paramount. This fact leads to the following question: is the Nation, with its critical infrastructure, sufficiently prepared to face a major event? More specifically, if a crisis occurred, could the country's CIKR prepare for it, respond to it, and restore itself to an acceptable level of functioning in a limited amount of time?

Just as vulnerability assessments have been used to better measure the abilities of individual facilities and CIKR Sectors to prevent and/or defend against a potential incident, a similar process is needed to measure their resilience. To help address this need, a resilience index (RI) has been formulated by Argonne National Laboratory in partnership with DHS to capture the fundamental aspects of resilience (i.e., robustness, rapid recovery, and resourcefulness) for CIKR assets, with respect to different types of threats. This index will generate reproducible results that can support decision-making related to risk management, disaster response, and maintaining business continuity and will also complement the vulnerability analysis that was developed and is currently being used by DHS.[2] The main objective of the RI is to analyze the ability of a critical infrastructure system to reduce the magnitude and/or duration of disruptive events. This index also allows assets to consistently prioritize the investments they make in their infrastructure in order to improve their resilience. To accomplish these goals, Argonne developed a methodology that allows CIKR to be compared in terms of resilience, and ultimately in terms of risk.

Information must be accurate and transparent if it is to yield an effective RI that can be compared with other RI values. Reproducibility is especially critical because an index loses value if it cannot be compared and interpreted in a consistent manner. The site visits carried out under DHS's Enhanced Critical Infrastructure Protection (ECIP) program support the collection of accurate information that is used to compare CIKR in terms of their vulnerability, resilience, and ultimately, consequences and overall risk. Based on a questionnaire encompassing more than 1,700 data points, the program is appropriate for a wide range of CIKR facilities. The ECIP questionnaire allows the pertinent information that

(Continued on Page 4)

[1] U.S. Department of Homeland Security, *Critical Infrastructure and Key Resources*, (Washington, D.C.: 2010), available at http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

[2] Argonne National Laboratory, *Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program*, ANL/DIS-09-4, Decision and Information Sciences Division, (Argonne, Ill.: 2009).

Resilience Index *(Cont. from 3)*

characterizes a facility to be collected within a limited timeframe. The survey covers the existing protective and resilience measures in place at a facility by gathering data at the most vulnerable point for each measure (e.g., pipelines above ground). The data are then verified multiple times through a quality assurance (QA) review process. This QA process is an integral part of the larger methodology because it maintains the integrity of the information that was collected and the products that were disseminated. It does so by ensuring the data's validity and by decreasing the variance in the data collected at different sites. In addition, by "cleaning" the data before they are used to produce an RI score, the QA process reduces the overall time it takes to return a final product to the owners and operators.

The RI is based on the multi-attribute utility theory (MAUT). Resilience is decomposed into its individual attributes, which are then organized into an organizational tree. The resilience analysis organizes the information collected into five levels, in order of increasing specificity: raw data are combined into groups at Level 5, and the data groups are combined further through Levels 4 to 1. The RI combines three Level 1 components (robustness, recovery, and resourcefulness) that correspond to the resilience components defined by the National Infrastructure Advisory Council (NIAC),[3] twelve Level 2 components, and forty-seven Level 3 components that are defined by subject matter experts. Each question (raw data), and all components and subcomponents of the RI, is assigned a weight representing its importance relative to other questions/components/subcomponents in its grouping. The weights were obtained in accordance with the principles of "decision analysis," an approach that helps manage risk under conditions of uncertainty.[4,5] The methodology is based on a numerical representation of the value pattern by comparing different elements of a facility and by using the relationships "better than" and "equal in value to" to define their relative importance.

Another important element in this decision analysis tool is the transitivity of the ranking. This means that if Element A is more important than Element B, and Element B is more important than Element C, then logically Element A will be more important than Element C. This approach produces a relational representation of a facility's resilience alternatives by assigning a numerical value to each of its components. Value of each level component is obtained by using a weighted sum of its components in the level below. For example, robustness is determined by the weighted sum of its components (Level 2 of resilience): redundancy, prevention/mitigation, and maintaining key functions. By combining the different levels' values, the methodology allows obtaining a single value representing the resilience of the facility analyzed.

Although an individual RI is important with regard to the data it represents, it can be difficult to fully interpret. Without a frame of reference, the RI's value does not convey its full meaning. For instance, when there is no understanding of the other scores, does an overall RI score of 42 lead one to believe that a facility is quite resilient or to believe that possibly key resilience measures are lacking? Indeed, the value of an RI is strongly related to the specific type of sector and to the context of the facility's operating environment. A comparative framework is thus necessary. An individual score becomes more meaningful when it is compared with those within a set of similar facilities. Providing the owners and operators of a facility with a detailed analysis of its RI and a comparison across other similar facilities is useful; it provides perspective on where the subject facility stands relative to its peer group. The comparison can be made at the highest level (overall RI), next-highest level (e.g., robustness, Level 1), or numerous lower levels. The lower-level

(Continued on Page 5)

[3] National Infrastructure Advisory Council, *Critical Infrastructure Resilience, Final Report and Recommendations*, U.S. Department of Homeland Security, (Washington, D.C.: 2009), available at http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

[4] Keeney, R.L., *Value-Focused Thinking: A Path to Creative Decisionmaking*, Harvard University Press, (Cambridge, Mass.: 1992).

[5] Keeney, R.L., and Raiffa, H., *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, John Wiley and Sons, (New York, 1976).

Resilience Index *(Cont. from 4)*

comparisons provide good starting points for an owner and operator who is considering which resilience measures may be worthwhile to add. The higher-level comparisons provide a good indication of how the overall resilience posture at the facility compares to others within its peer group. To facilitate comparisons between different possible actions, Argonne has developed a Web-based tool, the ECIP Dashboard. This tool allows managers to change characteristics at each level and immediately see the potential changes to the overall values of the calculated indices by selecting possible options to consider. Instead of analyzing only one scenario, the Dashboard allows managers to consider as many scenarios as needed. This functionality reduces the uncertainty inherent in risk management by providing additional information to managers who are trying to determine the best way to ensure a better functioning, more resilient facility. The Dashboard provides different interactive windows that are particularly relevant to supporting decisions for proactive risk management. One of these windows is an RI scenarios screen that helps identify what resilience measures can be implemented (Figure 1).

At the top of the Dashboard screen, different tabs allow the selection of one of the three Level 1 RI parameters. The resourcefulness tab is subdivided into resourcefulness pre- and post-event. When one of these components is selected, the related Level 2 and Level 3 components appear in the middle of the screen, which enables the user to choose the different characteristics that apply to her/his facility. At the bottom of the screen, the user can see — in real-time — the repercussions of modifying these components in the different RI values that result. The capabilities of the Dashboard allow users to change parameters, speedily seeing results, and assess different scenarios. These capabilities make it a very powerful tool that is

(Continued on Page 17)

Figure 1: The RI Dashboard Screen

Recent U.S. Government Accountability Office (GAO) Reports Focus on Critical Infrastructure Resilience

by John F. Mortin,*
U.S. Government Accountability Office, Washington, DC

The United States has thousands of facilities that if degraded or destroyed by a manmade or natural disaster, could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to national well-being and governance capacity. DHS has overall responsibility for leading and coordinating the Nation's effort to protect CIKR. In doing so, DHS works with certain Federal agencies — known as Sector-Specific Agencies (SSAs) — that represent 18 industry Sectors, such as Commercial Facilities, Communications, Energy, and Transportation.

In June 2006, DHS issued the National Infrastructure Protection Plan (NIPP) to provide the approach for integrating the Nation's CIKR.[1] The Plan outlined the roles and responsibilities of DHS, SSAs, and other public and private sector partners in CIKR protection. The Plan also emphasized the importance of collaboration and partnering with and among the various partners and stressed reliance on voluntary information sharing between the private sector and DHS. DHS updated the NIPP in January 2009.[2]

Over the years preceding DHS's 2009 NIPP update, various stakeholders in Congress, academia, and the private sector began to question DHS's approach to critical infrastructure protection. CIKR partners expressed concerns that DHS had placed most of its emphasis on protection — actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with an attack or disaster — rather than resilience — which, according to DHS, is the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

The U.S. Government Accountability Office (GAO) recently completed two studies on DHS' efforts to incorporate resilience into its CIKR planning and operations. One study looked at how DHS and SSAs are incorporating resilience into planning. The other looked at how DHS is incorporating resilience into its field level interactions with CIKR owners and operators.

Incorporating Resilience into CIKR Planning

The first of two GAO's studies focused on DHS and SSA efforts to address the concept of resilience as part of their CIKR and Sector planning efforts. In March 2010, GAO reported that DHS's 2009 NIPP update had adopted resilience as a major theme by discussing it with the same level of importance as protection.[3] Whereas the 2006 NIPP primarily treated resilience as a subset of protection, the 2009 Plan generally referred to resilience alongside protection. According to DHS, these revisions were intended to (1) raise awareness about resilience as it applied to individual Sectors and (2) encourage more Sector and cross-Sector activities to address a broader spectrum of risks. The latter would include, for example, increased attention to cybersecurity — which can transcend different Sectors — and discussion of the importance of systems and networks within and among Sectors as a means of fostering resilience.

Following the publication of the 2009 NIPP, DHS issued guidance to the SSAs that discussed the issues DHS believed SSAs should consider for increased attention when

(Continued on Page 7)

[1] DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006).
[2] DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).
[3] GAO, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296 (Washington, D.C.: March 2010).

GAO *(Cont. from 6)*

developing their Sector-Specific Plans (SSPs).[4] DHS encouraged SSAs to emphasize resilience in guidance provided to SSAs in updating their plans. However, DHS was relying on the Sectors themselves to determine the importance of resilience in their plans. According to DHS, the balance between protection and resilience is unique to each Sector, and it must be recognized that the degree to which any one plan increases the emphasis on resilience will depend on the nature of the Sector and the risks to its CIKR. Sectors had not completed their plans at the time of GAO's review.

Incorporating Resilience into Interactions with Asset Owners and Operators

GAO's second study focused on DHS's efforts to incorporate resilience into its efforts to interact with asset owners and operators. In September 2010, GAO reported that DHS's actions to incorporate resilience into the programs that used to work with asset owners and operators had been evolving, but these efforts could be further improved if program management was strengthened.[5] In particular, DHS developed or updated programs to assess vulnerability and risk at CIKR facilities and within groups of related infrastructure, regions, and systems to place greater emphasis on resilience. However, it had not taken commensurate efforts to measure asset owners' and operators' actions to address resilience gaps. Furthermore, DHS had deployed more than 90 critical infrastructure protection and security specialists — also known as Protective Security Advisors (PSAs) — throughout the country to assist asset owners and operators on CIKR protection strategies. Although DHS provided guidelines to PSAs on key job tasks and training on resilience topics, it had not updated PSA guidelines to articulate the role of PSAs with regard to resilience issues, or how PSAs were to promote resilience strategies and practices among asset owners and operators.

GAO also reported that DHS faced barriers disseminating information about resilience practices across the spectrum of asset owners and operators. DHS shares information on potential protective measures with asset owners and operators and others, including State and local officials (generally on a case-by-case basis) after it has completed vulnerability assessments at CIKR facilities. Although DHS had considered ways to disseminate information it collected or planned to collect with regard to resilience, it faced challenges sharing information about resilience strategies. For example, given the voluntary nature of the CIKR partnership, DHS officials stated that DHS should not be viewed as identifying and promoting practices which could be construed by CIKR partners to be standards. Another barrier is differences from Sector-to-Sector — the need for and the emphasis on resilience can vary across different types of facilities depending on the nature of the facility. For example, an oil refinery is inherently different than a government office building. DHS officials agreed that disseminating information on resilience practices broadly across the CIKR community would be a worthwhile exercise but they were uncertain which organization within DHS would be responsible for doing so.

Conclusions

DHS has increased its emphasis on critical infrastructure resilience in the NIPP and has adopted resilience as a major theme by discussing it with the same level of importance as protection. Consistent with these changes, DHS has also taken actions to increase its emphasis on resilience in the programs it uses to help asset owners and operators identify resilience characteristics and gaps. These actions could be improved if DHS were to develop measures to assess the extent to which asset owners and operators are taking actions to address resilience gaps identified during vulnerability assessments; and updating PSA guidelines to articulate PSA roles and responsibilities with regard to

(Continued on Page 21)

[4] The NIPP depends on supporting Sector Specific Plans for full implementation within and across CIKR Sectors. Sector-Specific Plans are developed by SSAs in close collaboration with Sector partners and contain the plan to identify and address the risks to CIKR specific to each Sector.

[5] GAO, *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving, but Program Management Could be Strengthened*, GAO-10-772 (Washington, D.C.: September 2010).

Mitigating Disruptions through Organisational Resilience

by Rita Parker, ISSR, Australia
Distingushed Fellow, CIP/HS
Visiting Fellow, Australian Defence Force Academy, University of New South Wales, Canberra

Embracing resilience is a logical step as part of a strategy to mitigate the unprecedented set of disruption and catastrophic events which have increased the challenges of the 21st century. Traditional risks and threats have been compounded by the global financial crisis, climate change, cyber attacks, pandemics, increased piracy, dependency on technologies, and threats to energy availability and to supply chains.

Intentional acts of disruption can include industrial action, strikes, sabotage, theft, and computer hacking. In 2009, the Federal Bureau of Investigation (FBI) ranked cybersecurity as the third greatest threat to the United States security after nuclear attack and weapons of mass destruction. Intentional acts also include acts of terrorism and piracy, which are carried out by non-state actors and, increasingly, by unaligned individuals.

Kangaroo in flood water, Queensland. *Photo courtesoy of Library.thinkquest.org.*

Accidental disruptions can also add to an uncertain operational environment and can include mechanical and technical failure, cuts to power supplies, food and water contamination, and chemical spills.

By definition, disruptions are difficult to anticipate and hard to predict. Often, they begin to unfold before they are noticed and can have unforeseen consequences. The fact is, any disruption, whether natural, intentional, or accidental has the potential to impact nations, corporations, communities, and individuals. The degree to which they are affected is determined by their ability to cope. That is, their level of resilience maturity.

In a country known for bushfires and drought, the Australian State of Queensland experienced the worst floods in 35 years in January of this year. Three-quarters of the State was declared a disaster zone as the floods covered an area the size of France and Germany

Ingram Queensland, Jan 2011. *Photo courteosy of Townsville Bulletin.*

combined and 28,000 homes were without power in that one State.

Yet, unlike the floods in Brazil during the same month which claimed over 600 lives, at the time of writing, there were 20 fatalities and 12 people missing in Queensland. Exactly one week after the floods peaked in Queensland, the clean up was well under-way with thousands of volunteers working next to emergency personnel. People began to return to work as businesses resumed operations and public transport operated a free service to keep private vehicles to a minimum. Fruit and vegetable markets resumed, albeit with limited supplies. The people and State of Queensland have been described as "resilient" in the national and international media and by

(Continued on Page 9)

Org. Resilience *(Cont. from 8)*

politicians.

Shared Responsibility

Organisational resilience is the critical nexus between national and community resilience in mitigating disruptions. Each is, in some way, dependent on the other because resilience demands partnerships and interdependencies within and across social, corporate, and national boundaries. Each element in this complex network can have an importance out of proportion to its apparent relevance. Resilient organisations are pivotal for a nation's security, progress, and well-being, especially when the future is uncertain and likely turbulent.

Governments, communities, and organisations have separately embraced the concept of resilience as well as the path of a holistic, systemic approach and integration of previously disparate elements. In Australia, the resilience framework is societal. This recognises the interdependence between individuals, communities, and organisations. When speaking at the National Security College in June 2010, the Australian Federal Attorney-General, the Honorable Robert McClelland said, "[b]uilding resilience essentially means building relationships and forming partnerships."[1]

Although we are seeing an increasing number of partnerships and recognition of inter-dependencies within and between sectors, there are still significant gaps.

Figure 1: Resilience – A Shared Responsibility Diagram © ISSR 2010

Resilience Continuum

Organisations have the potential to provide an existing systemic contribution to a holistic resilience continuum to mitigate disruptions. But, this requires the integration of organisations into the resilience planning of both nations and communities.

Public-private partnerships are integral to the development of resilience for a nation's security, its well-being, and to mitigate disruptions. Protection of national assets such as transportation hubs, bridges, water and power supplies, communications facilities, and supply chain networks are critical for a nation's security, its economy, and its future as a trading nation. Infrastructure, increasingly in private ownership, should be an enabler of national security, prosperity, and progress; infrastructure should *not* be a nation's Achilles heel. Direct collaboration between government and critical infrastructure owners and operators and the wider business sector is a cornerstone of building resilience to mitigate disruptions which has yet to be fully realised. The United States National Infrastructure Advisory Council report (2009) noted that, "it is essential for government to change the way they prepare and partner on resilience efforts, especially in our increasingly interconnected world."[2]

The Council noted that collaboration on resilience must be based on true partnerships of equals

(Continued on Page 10)

[1] Honorable Robert McClelland, Federal Attorney General, Community Resilience and National Security: An Agenda for the Future, National Security College, ANU, (June 13, 2010).

[2] National Infrastructure Advisory Council, *Critical Infrastructure Resilience: Final Report and Recommendations*, U.S. Department of Homeland Security, (September 8, 2009), 22.

Org. Resilience *(Cont. from 9)*

and not merely presented as an implicit threat of regulation.

Increasingly, numbers of corporations have recognised the benefits of building organisational resilience by aligning strategy, operations, management systems, governance structures, and decision support capabilities. In this way, organisations are in a better position to uncover and adjust to continually changing routine and non-routine risks, to endure disruptions and create advantages over less adaptive competitors or adversaries, and to fulfill their roles as contributors to national resilience and social well-being. In fact, following a disruption, an organisation with a higher degree of resilience can use the event as an opportunity to improve its effectiveness, enhance its reputation, and increase staff morale. In turn, that organisation has the potential to augment its community standing.

Governments are increasingly seeking better ways to work with communities, particularly in areas prone to natural disruptions, such as hurricanes and floods. There is greater consultation by governments, at the Federal, State, and local levels about what communities need and there is increasing provision to influence public policy development.

Disconnection in the Resilience Continuum

However, what is often missing in responses to disruptions is the involvement of organisations which deliver services to communities *or* which own and operate facilities which are *not* identified as critical infrastructure but upon which communities rely and governments implicitly include in their planning, such as dairies, media outlets, freight distributors, etc. It is the modern version of the butcher, the baker, and the candlestick maker.

As we develop the concept of resilience across national, corporate, and social boundaries, inherent interdependencies become clearer and the gaps more obvious. Ideally, each sector or element should be connected to and contributing towards the resilience of the other. It should be a seamless continuum for the delivery of essential services, to drive economic growth, to support social needs, and to support the economic performance and well-being of each nation and its people. But, with a single point of failure or failed integration, the entire system can fail. The weakest point at this time is disconnection through the exclusion of the majority of medium and small organisations in the resilience continuum. This single point of failure can impact the entire resilience continuum if not remedied and mitigation strategies will not be fully realised.

It is easy to perceive organisations as large detached entities, of relevance only to the stock market and shareholders, or to remote boards of directors. But organisations are not passive entities. They are made up of people and, like Alistair Mant's[3] story of the frog and the bicycle, organisations work best when all the parts are connected. In this instance, that means connections within the organisation and with the community in which it is located and which, more broadly, it serves — because an organisation operates as an open system. The people who work in organisations live in communities. Logically, therefore, there should be no disconnection in the resilience continuum.

Organisations are made up of the same people critically affected by the level of, or absence of, community resilience. They depend on a workforce at home or abroad, which is sufficiently resilient to provide the means of production or the services which in turn determine their contributions to resilience as part of the continuum to achieve national resilience.

Resilience tends to increase if an organisation has diversity, redundancy efficiency, agility and flexibility, autonomy, strength of its critical components — including its people and strong connections with its stakeholders. This allows it to continue to function if a link is broken, if a particular resource becomes scarce, or if a particular decision-maker or leader is unavailable.

For the resilience continuum to be truly effective, there needs to be a holistic, integrated, and inclusive process which recognises and benefits from the inter-relationship

(Continued on Page 21)

[3] Alistair Mant, Intelligent Leadership, (Allen and Unwin), 1997.

Risk Management and Resilience

by John J. Brown, PE, Director, Risk Management, Supply Chain Development,
The Coca-Cola Company

Resilience. A popular term today, especially with consultants and standards-setting organizations. Resilience fits into the same class as the terms *risk appetite*, *speed of onset*, and *risk intelligence*. These terms invoke emotional reactions and emotional connections. They also resonate with senior management. But, are they useful to advance or improve an organization's ability to survive and thrive? Not likely, at least as they are used today.

As explained in this article, resilience is the result of effective risk management. As far as the other terms, *risk appetite* is evidenced in policies and procedures implemented in response to potential risks, and generally involve some level of real-time judgment guided by a risk philosophy. Outside the financial world, it is difficult to succinctly state the amount of risk an organization is willing to accept. *Speed of onset* must be factored into how a potential risk is treated, but is not a factor to determine level of risk and risk prioritization as some consultants propose. And *risk intelligence*? This is the outcome of effective risk management.

Defining Resilience

Let us take a look at the word resilience. The term resilience is defined by dictionary.com as:

1. The power or ability to return to the original form, position, etc., after being bent, compressed, or stretched; elasticity; and

2. Ability to recover readily from illness, depression, adversity, or the like; buoyancy.

The on-line Merriam-Webster dictionary defines resilience as:

1. The capability of a strained body to recover its size and shape after deformation caused especially by compressive stress; and

2. An ability to recover from or adjust easily to misfortune or change.

Visions of palm trees bending against gale-force winds come to mind, or perhaps a linebacker bouncing off two opposing team members before continuing downfield to a touchdown. These are nice visuals, and we can connect with the concept, but what does resilience mean within an organization and how do we obtain this state of being?

Let us take a look at another definition for resilience. International Organization for Standardization (ISO) Guide 73:2009 defines resilience as "adaptive capacity of an organization in a complex and changing environment." Not quite as thought-provoking as the others, but probably closer to reality.

Being resilient simply means being able to assess (identify, analyze, and evaluate) and treat potential risk events. It is nothing more, nor less, than risk management (see ISO 31000:2009 Risk Management: Principles and Guidelines for a pragmatic risk management framework, Figure 1 on page 12). It is conceptually simple, but difficult to effectively put into practice. Why? It is because assessing potential risk events is part science, part art, and determining how to treat a potential risk event involves multiple factors that must be balanced against organizational resources and objectives.

Risk Assessment

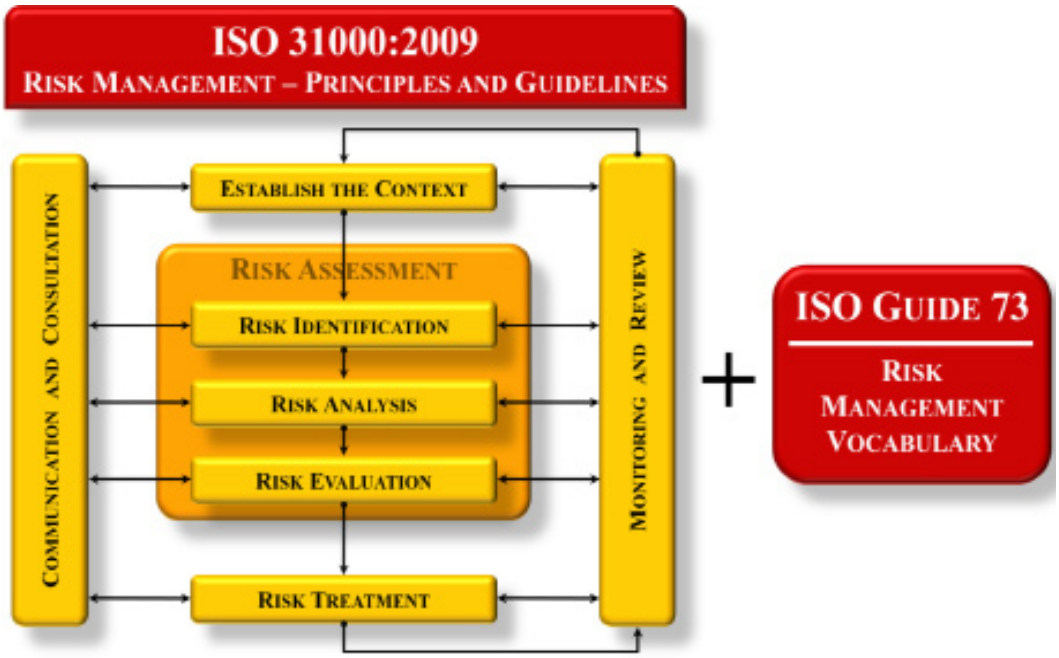
As human beings, we are hampered by psychological biases. Risk events that occurred in the recent past loom much larger than those that happened one or more years ago. Our frame of mind at any given moment clouds our ability to objectively identify and analyze risks. The path of our career and our lives impacts the way we view the world and how we perceive risks. Our educational background

(Continued on Page 12)

Risk Management *(Cont. from 11)*

and business environment affects the scope of our view into risks. Why is this important to resilience? We are likely to fail to identify a risk event that impacts our organization, or we underestimate its significance. By failing to identify a significant risk event, we have not taken action to reduce the likelihood of the event or minimize the magnitude of consequences (if the consequences are positive, we want to increase the likelihood and maximize the magnitude of consequences). We thus leave our fortune to luck. This is not a good way to run an organization.

Figure 1: Foundation for Resilience: Solid Risk Management Framework Coupled with Standard Technology.



How can we overcome the problems with risk assessment? Two techniques work well, and both are needed. First, involve individuals from multiple functions and multiple levels in your organization, and use group discussions to overcome individual, functional, and organizational level biases. Second, make risk assessment a frequent, on-going process, not a one-off spot-in-time exercise.

Risk Treatment

Assuming we have been successful in identifying potential risk events and those that are significant, how we deal with these risks is an equally critical process.

Risks can be classified broadly into two areas: risks to strategy, and operational risks. Operational risks are those over which we generally have direct control, such as producing a quality product or service, costs to manufacture, compliance with legal and internal requirements, and employee performance management. Risks to strategy are risks over which we have little direct control, such as competitor actions, public perception, and economic conditions. This distinction is important because it affects the way we treat the risks.

Emerging or unknown risks represent a third area. These risks, once known and defined, will fall into the strategic risk world or the operational risk world.

When risk treatment is being investigated, it is also important to realize that risk events have two dimensions: likelihood of occurrence, and magnitude of consequences. We want as much as possible to concentrate on the likelihood dimension, since prevention provides a greater return on investment. Most operational risks are best treated by minimizing the likelihood of occurrence.

Treating risks to strategy requires a modified, slightly different approach. As stated above, we have little direct control over the likelihood of these risks, and generally there are multiple potential consequences. So what do we do? Wait for a risk event to happen and then deal with it? Yes... and no.

Early Detection/Rapid Response

This is where resilience is developed. Using scenario analyses techniques, potential strategic risk events and how they could play out are explored. A range of likely scenarios is agreed, and response actions

(Continued on Page 18)

The Need for Including Critical Infrastructure Resilience Capability in United Nations Counter-terrorism Capacity Assessments

by Prof. A. Kumar

This article underscores the need to include critical infrastructure resilience as part of the counter-terrorism assessments conducted by the United Nations (UN) under United Nations Security Resolution 1373 (UNSCR 1373) and its successor resolutions. The first section examines the broad criteria used in counter-terrorism assessments currently undertaken by the United Nations on the country level. The second section delves into the types of policy measures relating to critical infrastructure resilience that a number of national governments have implemented and the priority that they have accorded to this salient area of homeland and national security. The third section briefly discusses the current use of the word "resilience" in the UN domain. The fourth and concluding section discusses the need to include an assessment of critical infrastructure resilience in counter-terrorism assessments that are undertaken by the UN 1373 Counter Terrorism Regime.

Broad Provisions of Counter-Terrorism Capacity Assessment Criteria Currently Used by the United Nations:

The UN Counter Terrorism Committee, or the UN 1373 Committee, passed Resolution 1373 in 2001.[1] Through a subsequent resolution passed in 2004, the Security Council has tasked the Counter Terrorism Executive Directorate (CTED) to assist the Counter Terrorism Committee (CTC) in assessing the counter-terrorism capacities of Member States by evaluating their compliance with the broad provisions of UNSCR 1373 and its successor resolutions. These provisions pertain to counter-terrorism legislation, counter-financing of terrorism, law enforcement, border control, and international cooperation. While these areas of counter-terrorism capacity assessment are undoubtedly of great importance, it is crucial that these assessments also include an evaluation of counter-terrorism capacity relating to critical infrastructure resilience. CTED also arranges for technical assistance to redress such counter-terrorism capacity deficits.

Importance Accorded to Critical Infrastructure Resilience by Member States

The 2009 NIAC final report defines infrastructure resilience as the ability to reduce the magnitude, impact, or duration of a disruption. The report further defines resilience as the ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. It offers the following prescriptions relating to critical infrastructure resilience: (1) fortify government policy framework to strengthen critical infrastructure resilience; (2) improve government coordination to enhance critical infrastructure resilience; (3) clarify roles and responsibilities of critical infrastructure partners; (4) strengthen and leverage public-private partnership; (5) encourage resilience using appropriate market incentives; and (6) implement government enabling activities and programs in concert with critical infrastructure owners and operators.[2] The government of Singapore has adopted a whole-of-government approach to translate potential risks and challenges to critical infrastructure into resilience frameworks, structures, and processes including, quite significantly, those concerning the domain of counter-terrorism. In December 2009, at the meeting of the Critical Infrastructure Advisory Council (CIAC), the government of Australia announced its intention to shift their existing Critical Infrastructure Program to Critical Infrastructure Resilience.

(Continued on Page 19)

[1] Please see the website of the UN Counter Terrorism Committee accessible at http://www.un.org/en/sc/ctc/.
[2] Accessible at http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

Legal Insights

Volunteer Health Care Provider Liability Protections and Registration Services: Critical Support for Response Efforts during a Public Health Emergency

by Jalayne J. Arias, J.D.*

The response infrastructure necessary during a disaster, emergency, or public health emergency[1] is dependent upon medical professionals to provide critical services. Volunteer health care providers (VHPs) offer necessary relief in response to increased demands on health care facilities and medical professionals during an emergency. During an emergency, health care facilities and providers face a surge of patients and demands, a limitation of resources (e.g., staff shortages and limited medical supplies), and severe working conditions (e.g., loss of power). [2] These circumstances may limit a health care provider's ability to deliver medical care through traditionally accepted methods. Such limitations may raise VHPs' concerns regarding civil liability for actions or inactions taken in the immediate aftermath of or during an emergency. Law, however, can provide necessary support to alleviate or mitigate health care providers' liability concerns. Protections available in Federal and State law support VHP services critical to the emergency response infrastructure.

Protections found in Federal and State law allow VHPs to react in real-time to the environment they are in, rather than hold them to expectations found in traditional circumstances. Real-time reactions may require VHPs to make decisions without full information about the patient seeking treatment. For example, a physician administering pain medication may lack knowledge of other medications currently taken by the patient. Traditionally, this would expose the physician to a negligence claim stemming from an adverse drug reaction. However, under various statutory provisions, a VHP may be protected as long as the VHP acted without gross negligence, willful misconduct, or criminal intent. The protections may reduce a VHP's hesitance to respond in circumstances that require actions traditionally outside the standard of care.

As indicated, the legal environment during an emergency, whether or not a state of emergency has been declared, can shape response efforts. The legal environment includes an imbedded risk of civil liability for injuries and deaths resulting from medical care. Traditional medical professional civil liability is generally determined through the standard of care. This standard indicates that a physician[3] is liable for an injury or death if the care provided is below the level of care that would have been provided by a reasonable physician acting in like circumstances.[4] Several key types of protections found in State and

(Continued on Page 15)

[1] States differ on the use of the terms "emergency," "disaster," and "public health emergency." However, a majority of States define these terms to include natural disasters (e.g., Hurricane Katrina), human caused disasters (e.g., September 11th), and epidemics (e.g., 2009 H1N1 epidemic). For purposes of the article the term emergency will include "disasters" and "public health emergencies." For examples of varying definitions see Emergency Management, "Definitions," Arizona Revise Statutes Annotated § 26-301 ("Emergency"); Emergency Management, "Definitions," Texas Government Code Annotated § 418.004(1), (3) (Vernon 2003) ("Disaster"); Emergency Management Agency, "Definitions," West's Smith-Hurd Illinois Compiled Statutes Annotated § 3305/4 ("Public Health Emergency") (2007).

[2] "Hurricane Katrina's Deadly Legacy at Memorial Medical Center," *Fox News*, August 27, 2010, accessed January 14, 2011, http://www.foxnews.com/health/2010/08/27/hurricane-katrinas-deadly-legacy-memorial-medical-center (interview with Dr. Anna Pou regarding conditions during the aftermath of Hurricane Katrina).

[3] Similar standards apply to other medical professionals, including nurses.

[4] Philip G. Peters, "The Quiet Demise of Deference to Custom: Malpractice Law at the Millennium," *Washington and Lee Law Review 57* (2000): 163-205.

Legal Insights *(Cont. from 14)*

Federal laws offer support to VHPs who may not have otherwise met this standard while providing medical services during an emergency. Each protection differs in the applicability, coverage and limitation provided within the law. Such protections include: (1) volunteer protection acts; (2) Good Samaritan laws; (3) governmental immunity; and (4) emergency laws.

Volunteer protection acts, including the Federal Volunteer Protection Act, have the broadest applicability. The Federal Volunteer Protection Act provides protections to volunteers working "within the scope of the volunteer's responsibilities."[5] Similar protections are available at the State level.[6] These statutory protections provide protections regardless of the status of an emergency, and therefore protect health care providers even where an emergency has not been declared. The applicability of this type of protection is limited by restricting protections to volunteers providing services for non-profit organizations, hospitals, or government organizations.

More limited protections are available through Good Samaritan laws and governmental immunity. Similar to volunteer protection acts, governmental immunity laws and Good Samaritan laws do not require a declared emergency. However, they include further restrictions regarding the circumstances or individuals to which they apply. For example, most Good Samaritan laws only apply if a VHP responds to an emergency where services were not prearranged. These statutes generally seek to reduce the standard of care for volunteers who provide services at the scene of an emergency (e.g., providing medical treatment at the scene of a car accident prior to emergency services arriving).[7] Among the protections discussed in this article, Good Samaritan laws apply to the fewest circumstances. In the emergency response infrastructure, a Good Samaritan law may only apply if a VHP provides care at the scene of a single incident (e.g., a hurricane or an earthquake) immediately after it has occurred.

Conversely, governmental immunity laws may apply in a multitude of circumstances, but they are severely limited to the group of individuals they protect. Governmental immunity is generally limited to employees or agents of the State (and potentially for limited types of actions).[8] In a number of States, VHPs do not fall within the definition of employees or agents of the State. However, in other States, volunteers may be deemed employees of the State in limited circumstances.[9] Where volunteers are included within the definition, governmental immunity may have a broader impact. However, limitations are still imbedded in requirements that the volunteer must be acting on behalf of the State. Despite this limitation, governmental immunity offers the distinct advantages of allowing for compensation (unlike volunteer protection acts) and for VHPs to be prearranged (unlike Good Samaritan laws).

Lastly, emergency statutes may provide an additional protection to VHPs providing services in response to a declared emergency.[10] The limitation of the effectiveness of these statutes is dependent on the public official with the authority to declare an emergency or public health emergency. For example, only a minority of States declared a state of emergency or public health

(Continued on Page 20)

[5] Volunteer Protection Act, 42 U.S.C. § 14503(a).

[6] *See* "Qualified Immunity," Arizona Revised Statutes § 12-982 (providing protections for a volunteer providing services for nonprofit organizations, hospitals, or government entities).

[7] *See* Vernon's Texas States and Codes Annotated, Civil Practice & Remedies Code §74.151 (2007) ("A person who in good faith administers emergency care is not liable in civil damages for an act performed during the emergency unless the act is willfully or wantonly negligent" where a emergency is defined as the "sudden onset of a medical or traumatic condition.")

[8] "Qualified Immunity," Arizona Revised Statutes § 12-820.02 (protect public employees from liability for limited circumstances, including failure to make an arrest and similar types of actions and inactions).

[9] "Governmental immunity from Tort Liability," Michigan Compiled Laws Annotated § 691.1407 ("each volunteer acting on behalf of a governmental agency [. . .] is immune from tort liability for an injury to a person or damage to property caused by [. . .] the volunteer while acting on behalf of a governmental agency.").

[10] *See* "Privileges and Immunities," Arizona Revised Statutes § 36-790 ("A person or health care provider [. . .] is immune from civil or criminal liability if the person or health care provider acted in good faith.").

Resilience *(Cont. from 2)*

way of life. While we continue with our own activities, we can also work collaboratively within communities, industries, and organizations to ensure that we are prepared for adverse events (natural, manmade, or terrorist), whether that preparation reduces the likelihood of such events or minimizes their consequences. There is limited benefit to distinguishing between improvements in protection versus resilience at the overall level. However, individual programs and efforts may be targeted at one or the other and that is fine so long as they are communicating.

We can and should continue to build on approaches that work for our unique needs — we do not all have to use exactly the same approach or even vocabulary to obtain the desired benefits. If we force people, organizations, and institutions to change approaches and language, they may stop doing the effective approaches that are working today. Most important, in order to meet new expectations and requirements, they may stop utilizing approaches that are integrated into their operations. This is the last thing we want, as approaches that are integrated into operations are those that have proven their worth over time — meaning that individuals, companies, or government organizations think they are important to sustain and invest in over time. Thus, we want to identify opportunities to take these effective practices and approaches and leverage them over a larger area or set of businesses/agencies, or even across industries and sectors.

Resilience will often involve coordinating with others outside an organization (private or public) and can involve sharing sensitive information with these parties. Therefore, it may require the engagement of more senior management than might be necessary for more straightforward decisions about the protection of an organization's own assets, systems, or people. Given the varied demands on senior management's time, it is even more important to follow the practices and use the vocabulary to which they are accustomed. For instance, there is no need to force them to call something resilience if they already think of it in terms of business continuity. On the other hand, re-labeling business continuity efforts as part of a new resilience initiative could breathe life into a plan or effort that has not been widely accepted within an organization. We should have the flexibility to leave well enough alone or to change our approaches where needed, all in the name of improving resilience.

The important thing is to make the cultural shift, primarily by realizing that we are all striving for common goals and that we are well on our way; this is not a new burden that we must address. It is part of good business, good government, and individual preparedness and most of us are already doing various things that will make us a more resilient society. We just need to do more of them, and do them more efficiently.

The rest of this issue includes discussions of resilience from a number of different perspectives and environments. Yet they all fit together to improve different aspects of our infrastructure and our society. We should seek to identify and transfer best practices and insights from one area to another. ❖

Resilience Index *(Cont. from 5)*

particularly relevant with regards to managing risk-related decisions concerning critical infrastructures. Facility-specific RIs demonstrate the potential effects of prioritizing measures for a particular facility. The list of common options, identified through comparisons with those of other similar facilities, can help managers make decisions regarding a site-specific resilience strategy.

It is important to note that no two facilities are alike. Each facility's safety staff and management team must determine the appropriate combination of measures on the basis of their own assessment of risks, which considers the threat, specific assets to be protected, consequences, overall vulnerability, facility characteristics, business impacts, return on investment, and overall resilience. The information from the RI and the ECIP program methodology, however, gives them consistent insights into elements of resilience as well as other aspects of CIKR risk.[6]

In the context of a complex and interconnected world, it is important to reinforce the protection and increase the resilience of CIKR. Critical infrastructure networks support the well-being of society. It is essential to support the owners and operators of critical infrastructures with tools that allow them to analyze risk in a comprehensive way and that present them with different alternatives to manage this risk. The development of the RI is intended to help DHS analyze the resilience associated with the Nation's CIKR and identify ways that might improve it. This index complements previously developed vulnerability assessments designed to enhance the current ECIP program. In addition, the index can give facility owners and operators valuable information on their standing relative to similar sector assets as well as on ways to increase their overall resilience.

The applications and uses of the RI for the ECIP program will continue to evolve, concepts will continue to improve, and enhancements and approaches will continue to be added. Combining the RI with other indices will provide additional benefits, allowing for a better overall view of risk. The continual objective is to develop better decision-making tools that will enable the comparison of critical infrastructures and promote a proactive approach for improving their robustness, resourcefulness, and recovery capabilities. ❖

[6] Fisher, R.E., and Petit, F.D., 2010, *Applying Appreciative Inquiry to Facility Security Decision Making*, presented at Third International Conference and Doctoral Consortium on Organization Development and Change, Institut de Socio-Economie des Entreprises et des Organisations (ISEOR), Jean Moulin University, Lyon, France, June 14–16.

Risk Management *(Cont. from 12)*

formulated. Then, possible triggers for the risk events are identified and monitored. As soon as a risk event trigger is detected, the response plan is initiated. Rather than reducing the likelihood of a strategic risk event, we focus on detecting when it starts. Reducing the magnitude of consequences is accomplished by knowing our response actions and being ready to put them into action as soon as the risk event starts.

Put simply, the above process prepares an organization for early detection and rapid response to strategic risks. The accompanying diagram illustrates the concept (see Figure 2). The earlier an event is detected, and the earlier the response is initiated, the less damage will occur. If executed well, and the risk event also affects the organization's competitors, these actions can result in an increase in organizational value at the expense of competitors.

Effective Risk Management Results in Resilience

Effective management of both operational risks and strategic risks is important to the success of an organization. Solid management of operational risks ensures the ship continues to move forward. Effective management of strategic risks ensures the ship is headed in the right direction and the crew is ready to respond to potential obstacles in the organization's path to achieving its goals. It does not do any good to be headed in the right direction if the ship is not moving, and conversely, it does not do any good for the ship to be moving if it is in the wrong direction or into an iceberg.

Resilience is gained by being able to quickly detect and rapidly respond to, potential strategic risk events while ensuring operational risks are well-managed. ❖

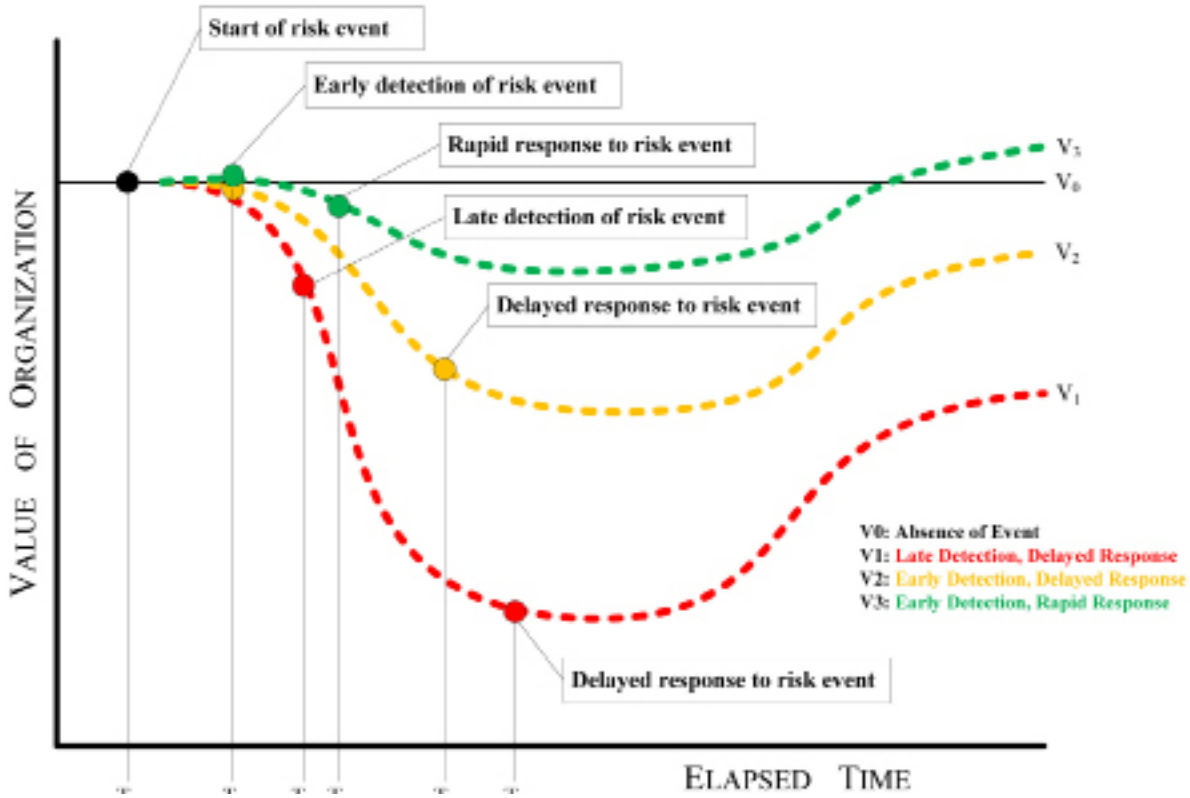


Figure 2: Effect of Event Detection Lag and Response Log on Organization Value.

UN Assessments *(Cont. from 13)*

This program will include organizational resilience and support for disaster resilience as its two prime components. Other governments have taken note of lessons learned in the aftermath of events like the 2005 London bombings and the 2008 Mumbai terrorist attacks on soft targets like hotels. Similarly, the governments of other Member States have taken steps to highlight the importance of critical infrastructure resilience in the counter-terrorism measures they employ.

Use of the Word "Resilience" in the UN Lexicon

The words "resilience" and "infrastructure vulnerability" are already a part of the UN lexicon. The UN's International Strategy for Disaster Reduction (ISDR) mentions the concept of Resilient Cities. Quite significantly, Pillar II of the United Nations Global Counter Terrorism Strategy calls for stepping up all efforts to improve the security and protection of particularly vulnerable targets such as infrastructure and public places. It also calls for improving the response to terrorist attacks and other disasters, particularly in the area of civil protection, while recognizing that states may require assistance to that effect. Furthermore, Pillar III of this Strategy encourages the United Nations to work with Member States and relevant international, regional, and sub-regional organizations to identify and share best practices to prevent terrorist attacks on particularly vulnerable targets; invites the International Criminal Police Organization to work with the Secretary-General so that he can submit proposals to this effect; and recognizes the importance of developing public-private partnerships in this area.[3] In an effort to translate this element of the Strategy into tangible action, the UN set up a Working Group on Strengthening Vulnerable Targets within the Counter Terrorism Implementation Task Force charged with implementing the overall strategy. This Working Group has been striving to identify, collate, and propagate best practices amongst Member States relating to public-private partnerships for protecting such vulnerable targets.

The Need to Include Critical Infrastructure Resilience as an Assessment Criterion in Evaluating Counter-Terrorism Capacity

Given the salience of critical infrastructure resilience and the increased focus that many Member States have placed on this aspect of national and homeland security, it is imperative that this becomes one of the criteria of the counter-terrorism capacity assessments undertaken by the Counter Terrorism Executive Directorate. Already, the CTED looks to the Financial Action Task Force (FATF) as the authoritative body for development and adoption of standards pertaining to terrorist financing; compliance with these standards is used as an assessment criterion by CTED to assess compliance with counter-terrorist financing measures. Security Council Resolution 1373 and its successor resolutions, including the most recent Resolution 1963, do not have critical infrastructure resilience as a part of the required assessment criteria for counter-terrorism capacity. While the United Nations Counter Terrorism Strategy does mention protection of vulnerable targets, as indicated earlier, the Security Council resolutions do not. It is important to note that the Counter Terrorism Strategy was passed by the United Nations General Assembly whose resolutions on security related issues are not binding. On the other hand, by virtue of Chapter VII of the UN Charter, Security Council resolutions are binding on Member States. The inclusion of suitable assessment criteria pertaining to resilience, such as the six elements mentioned in the 2009 NIAC report, could greatly enrich forthcoming Security Council resolutions of the UN 1373 Counter Terrorism Regime. Furthermore, it could result in a more comprehensive process to remedy any deficits in critical infrastructure resilience as part of the overall counter-terrorism capacities of Member States. ❖

[3] Accessible at http://www.un.org/terrorism/strategy-counter-terrorism.shtml.

Legal Insights *(Cont. from 15)*

emergency during the 2009 H1N1 epidemic.[11] VHPs in States without a declared state of emergency may not have been protected under those States' emergency statutes.

A movement to protect VHPs who are critical to effective response efforts is visible in the passage of laws[12] and the applicability of current laws to protect medical professionals responding to severe circumstances. While each protection has limitations, the combination of these protections allows VHPs to maintain a critical role in the infrastructure of emergency response efforts. ❖

**Jalayne J. Arias, JD is a fellow/faculty associate with the Public Health Law and Policy Program at the Sandra Day O'Connor College of Law, Arizona State University; and Deputy Director, Public Health Law Network - Western Region, Arizona State University.*

[11] Eleven States (California, Florida, Illinois, Maine, Maryland, Nebraska, New York, Ohio, Texas, Virginia, and Wisconsin) and American Samoa declared a state of emergency, public health emergency or made a similar declaration in response to the 2009 H1N1 epidemic. http://www2a.cdc.gov/phlp/h1n1flu.asp#dec.

[12] In addition to the discussed laws, a minority of states have adopted provisions of the Uniform Emergency Volunteer Health Practitioners Act ("UEVHPA"). UEVHPA delineates two alternative approaches to protecting health care providers from liability (excluding protections from actions which are willful misconduct, grossly negligent, or criminal). Uniform Emergency Volunteer Health Practitioners Act, accessed January 20, 2011, http://www.law.upenn.edu/bll/archives/ulc/uiehsa/2007act_final.pdf (since 2007 over a dozen states have enacted in some form).

GAO *(Cont. from 7)*

resilience during their interactions with asset owners and operators. Although DHS faces challenges overcoming barriers to disseminating resilience information and strategies among asset owners and operators, DHS is uniquely positioned to do so because it is the primary Federal agency responsible for coordinating and enhancing protection and resilience across the spectrum of CIKR Sectors. By determining the feasibility of overcoming barriers and developing an approach for disseminating resilience information, DHS could better position itself to help asset owners and operators consider and adopt resilience strategies, and provide them with information on potential security investments, based on the practices and experiences of their peers within the CIKR community, both within and across Sectors.

GAO recommended that DHS develop resilience performance measures and update PSA guidelines to discuss the role of PSAs regarding resilience issues. GAO also recommended that DHS assign responsibility to one or more organizations within DHS to determine the feasibility of developing an approach for disseminating information on resilience practices. DHS agreed and is taking actions to develop performance measures and update PSA guidelines but said that its components need time to further consider the information sharing recommendation and will respond at a later date. ❖

**The author, John F. Mortin, is an Assistant Director responsible for Critical Infrastructure Protection Issues with the Homeland Security and Justice Team at the U.S. Government Accountability Office. He can be reached at mortinj@gao.gov. For more information on the two GAO reports cited, please see* Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience *(GAO-10-296) at www.gao.gov/cgi-bin/getrpt?GAO-10-296 and* Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving, but Program Management Could be Strengthened *(GAO-10-772) at www.gao.gov/cgi-bin/getrpt?GAO-10-772.*

Org. Resilience *(Cont. from 10)*

between all stakeholders — including organisations and communities. That is, a shared responsibility and mutual obligation between governments, organisations, communities, and individuals. It takes time and effort but the alternative can be devastating. In the words of Mahatma Gandhi: *we must become the change we want to see.* ❖

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

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