THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

AUGUST 2013
HEALTH

VOLUME 12 NUMBER 2

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

Follow us on Twitter here
Like us on Facebook here

This month *The CIP Report* highlights critical infrastructure security and resilience in the Healthcare and Public Health Sector. Articles examine issues ranging from cybersecurity and resilience planning to infectious diseases and biosecurity funding.

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

First, David G. Henry and Justin Snair of the National Association of County and City Health Officials discuss the risks of cyber attacks on the Healthcare Sector. Next, CIP/HS's own Melanie Gutmann addresses the dangers posed by infectious disease in the context of rapid globalization. Then, CIP/HS Research Associate Jassandra Nanini, J.D., analyzes the potential effects of reduced biosecurity funding on U.S. critical infrastructure security and resilience. Dr. Elvira Beracochea of MIDEGO, Inc. then explains the importance of local, national, and global coordination in establishing critical health infrastructure throughout the world. Finally, Anna Bethke, Dave Brannegan, and Kelly Wallace of Argonne National Laboratory evaluate hospital resilience in terms of operational dependencies, planning, and physical design.

We would like to take this opportunity to thank the contributors to 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. As always, thank you for your support and feedback.

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

Risks of Cyber Attacks on the Healthcare Sector Leave Public Health of Communities Vulnerable

by David G. Henry and Justin Snair,*
National Association of County and City Health Officials

The nation's Healthcare Sector has critical vulnerabilities resulting from increased reliance upon technology dependent operations. That reliance poses a risk to the security and well-being of our communities. While opportunities to improve patient care and health outcomes through information technology are important, current policy fails to address critical healthcare information technology security needs. Cyber attacks on healthcare facilities compromise more than patient privacy, but could also cause utility failures that can shutdown facilities. This risk, combined with existing known vulnerabilities within healthcare, such as surge capacity, hospital closures, and nurse shortages, create an immediate need for healthcare vulnerabilities to be addressed in national policy provisions on critical infrastructure, health security, and cybersecurity. Without a resilient Healthcare Sector, the overall public health of the community is at risk.

Healthcare infrastructure is already vulnerable, as our healthcare delivery system routinely operates at or near 100 percent of capacity on a daily basis.[1] The types of these systems under daily stress include public and private hospitals, emergency departments, and other in/outpatient facilities. Compounding the stress on the system is the increase in the aging U.S. population and rise in hospital admissions due to the impacts of hospital closures, the use of emergency departments as a primary point of care for the uninsured, and increased length of stay due to rising chronic illness rates in recent years. In addition, close collaboration among public, private, and non-governmental stakeholders to assure safe healthcare infrastructure is a challenge. Nearly 90 percent of healthcare facilities are privately owned and operated, and the majority of facilities have their own infrastructure and practices that occasionally cross sectors within the vast U.S. healthcare network.[2]

Public Health's Role

Private and non-profit healthcare delivery systems do not carry the burden of critical infrastructure protection alone. The public health sector—state and local health departments—are leaders within the Healthcare Sector to prepare for, respond to, and recover from man-made and natural disasters.

(Continued on Page 3)

[1] Smith, W. M., Institute of Medicine Forum on Medical and Public Health Preparedness for Catastrophic Events, "Financing Surge Capacity and Preparedness," 2009, http://www.iom.edu/~/media/Files/Activity%20Files/PublicHealth/MedPrep/Jun-10-11-2009-Commissioned%20Papers/Jun-10-11-2009-Commissioned-Paper-Financing-Surge-Capacity-and-Preparedness.pdf.
[2] The National Health ISAC (NH-ISAC) , August 9, 2013. http://www.nhisac.org/initiatives/.

(Continued from Page 2)

For local public health, healthcare is an equal partner in keeping the nation's health services secure for all communities. Public trust depends upon the sustainability and resilience of our national healthcare and public health critical infrastructure.[3]

Information Technology

Like all critical infrastructure and key resource sectors, healthcare does not operate in a silo. To resolve the aforementioned challenges of capacity, patient care, and public-private partnerships, the Healthcare Sector has turned to technology to share information, enhance efficiency, and improve patient flow and quality of care. To foster the improvements of the healthcare delivery system, federal doctrine, such as the *National Health Security Strategy* (NHSS), the Centers for Disease Control and Prevention's (CDC's) *Public Health Preparedness Capabilities: National Standards for State and Local Planning* (PHEP), and the U.S. Department of Health and Human Services' Office of the Assistant Secretary for Preparedness and Response's (ASPR's) *Healthcare Capabilities: National Guidance for Healthcare System Preparedness* (HPP) has promoted the adoption of technology in healthcare facilities. However, as healthcare providers begin to use e-Health, information technology and other web-based tools with inadequate security systems or enforcement, the sector opens itself to exposure to cyber threats. While the opportunities to improve patient care and health outcomes through technology are important and recognized in NHSS, PHEP, and HPP doctrine, the policies fail to adequately stress the importance of healthcare information technology security needs.

New Federal Doctrine and Policy

From the executive level, President Obama issued *Presidential Policy Directive (PPD)–21* and *Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity*, reinforcing the need for holistic thinking about critical infrastructure security and risk management. Those directives and executive orders will drive action towards critical infrastructure systems—including healthcare—to improve their network security. Additionally, those policies will help promote and incentivize the adoption of cybersecurity practices, increase cyber threat information sharing, evaluate and mature public-private partnerships, and understand the cascading consequences of infrastructure failures.

With the release of PPD-21 and EO 13636 and the subsequent operationalization of these policies, federal agencies responsible for NHSS, PHEP, and HPP should prioritize improving security of healthcare information systems, the strengthening of public-private partnerships vital to healthcare cybersecurity and resilience, and adopting standards and frameworks for information sharing and security within the revisions of guidance doctrine.

Cybersecurity: Implications for the Healthcare Sector

Without clear guidance, healthcare facilities are open to possible cybersecurity breaches. According to the Third Annual Benchmark Study on Patient Privacy & Data Security (2012), 94 percent of healthcare organizations have had at least one data breach in the past two years. However, 45 percent report that they have had more than five incidents.[4]

(Continued on Page 4)

[3] Ibid.

[4] "Third Annual Benchmark Study on Patient Privacy & Data Security." *Ponemon Institute LLC*, 2012, accessed August 9, 2013, http://lpa.idexpertscorp.com/acton/attachment/6200/f-0033/1/-/-/-/-/file.pdf.

(Continued from Page 3)

Cyber attacks on healthcare facilities can come in many forms. They can include not only breaches to patient records, but also disruptions from both sophisticated and uncoordinated attacks, such as unauthorized access of networked medical devices or malignant emails that may cause utility and power grid failures and other cascading failures across a facility. Power outages at hospitals, caused by the collapse of public power grids, cause hospitals to go off-line, and rely upon generator power. Both power transmission and power generation through infrastructure are often controlled by Supervisory Control and Data Acquisition (SCADA) systems—networked computer control systems that can monitor and control multiple components in and between facilities. As systems are linked over networks, the loss of power to a hospital through a cyber attack could include not only the failure of the computer system that manages the power grid, but the physical destruction of generators.[5] Critical Infrastructure Control Systems, such as Programmable Logic Controllers, are used for automatically regulating hospital environments and systems, and if disrupted would

have devastating consequences for patient care[6] and local communities.

In December 2011 a hospital in Georgia was forced to divert all non-emergency admissions to other medical centers after a malware infection downed the institution's IT network and required staff to use paper records. The attack affected computer connectivity, as hospital computers could not communicate with each other. The hospital was forced to use a runner system, where papers were shuttled by personnel from station to station.[7]

A cyber attack on a healthcare facility that disrupts its capacity to manage patients, combined with routine operation at or over capacity, could be devastating to a local community's ability to manage the routine care of its population, as well as patient surge during catastrophic events. The impact of cyber attacks on healthcare facilities can be organized into three categories:[8]

Losses of confidentiality: The exposure of personal data can trigger ripple effects for victims of cyber crime, including theft or loss of patient information. Another consideration is the connection between patient data and personal medical devices. Those devices carry security and privacy risks as they become increasingly networked and wireless.

(Continued on Page 5)

---

[5] Lemos, Robert, SecurityFocus, "DHS video shows potential impact of cyberattack," last modified September 27, 2007, accessed August 9, 2013, http://www.securityfocus.com/brief/597.

[6] Knapp, Eric, NitroSecurity McAfee, "Critical Control System Vulnerabilities Demonstrated (And What to Do About Them)," accessed August 9, 2013. https://files.sans.org/summit/euscada11/PDFs/Research Presentation- Critical Control Systems Vulnerabilities - And What to Do About Them - Knapp- 2 Dec 1515.pdf.

[7] Elliot, Richard. "Hospital put under 'Total Diversion' after computer virus," *WSBTV*, December 9, 2011, accessed August 9, 2013, http://www.wsbtv.com/news/news/local/hospital-diverting-trauma-cases-due-computer-probl/nFyYY/.

[8] Cyber Operations Cyber Operations and Cyber Terrorism," *US Army Training and Doctrine Command DCSINT Handbook 1.02,* 2005, accessed August 9, 2013, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA439217; Barnett, Daniel J., Tara Sell, Robert K Lord, James Terbush, and Thomas Burke, "Cyber Security Threats to Public Health,"*World Medical & Health Policy.* no. 1 (2013): 37-46, accessed August 9, 2013, http://onlinelibrary.wiley.com/doi/10.1002/wmh3.19/abstract.

(Continued from Page 4)

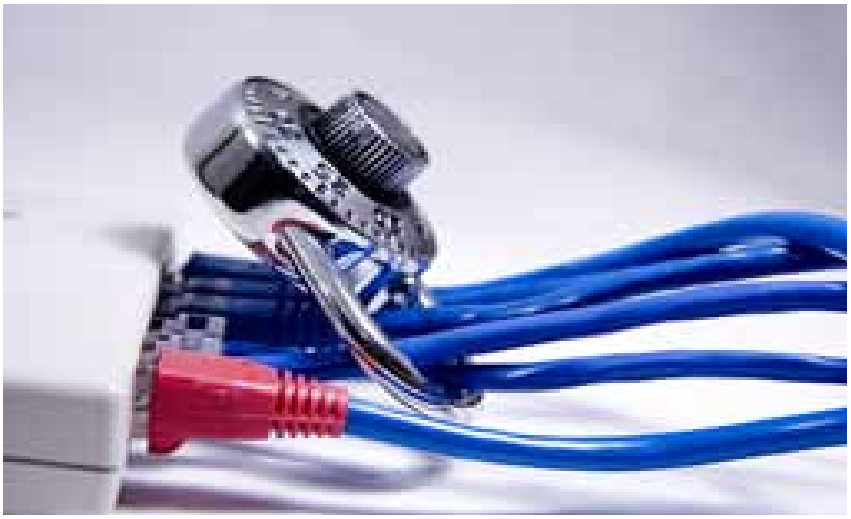
Losses of integrity: Patients and practitioners may lose confidence in a healthcare provider's ability to maintain patient privacy, due to perceptions of inadequate security.

Losses of availability: Cyber threats to data and operations systems can take a facility offline, leading to disruption of care due to software outages. In addition, the loss of access to health records may limit the provider's ability to provide appropriate care, shelter, and medicine in times of need. Lastly, damage to infrastructure—such as insurance and payment or utility systems—could also prevent people from accessing necessary medical care.

Conclusions

Preparing for, preventing, mitigating, and responding to the threat of cyber attack to healthcare facilitates requires a holistic approach. Successful planning involves coordination, communication, and cooperation among federal, state, local, tribal, and territorial governments, as well as healthcare facilities, medical device and equipment manufacturers, telecommunications and utilities providers, and medical supply chain operators. That coordination happens through public health leadership at the state and local levels. Until PPD-21 and EO 13636 are fully operationalized, healthcare critical infrastructure, and consequently local communities' capacity for resilience, are vulnerable.

Moving forward, local health departments and Healthcare Sector partners need not wait for revisions of federal doctrine or full implementation of PPD-21 and EO 13636 to begin improving the security of healthcare facilities. Communities can improve cybersecurity by opening a dialogue with the key local public-private stakeholders to improve partnerships and information sharing. Healthcare facilities can coordinate across sectors to engage technology experts to further improve system security and ensure the protection of their data and systems. Lastly, the Healthcare Sector can raise employee awareness of cyber threats by implementing digital hygiene training—meant to create a common understanding of how to keep computer systems safe. By making those first considerations to improve health information sharing and cybersecurity, Healthcare Sector operators can begin to reduce the risk and exposure that comes with the adoption of new technologies to improve their service delivery, patient care, and community resilience. ❖



**Mr. Henry and Mr. Snair are senior program analysts for public health preparedness at the National Association of County and City Health Officials (NACCHO)— the voice of the approximately 2800 local health departments across the country. NACCHO's mission is to be a leader, partner, catalyst, and voice for local health departments in order to ensure the conditions that promote health and equity, combat disease, and improve the quality and length of all lives.* *The authors thank Frances Bevington, Scott Fisher, Alyson Jordan and Andrew Roszak for their suggestions for this article.*

Globalization and Health Security

by Melanie Gutmann, M.S. Candidate, George Mason University

When considering issues of concern to national security and defense, the significant, but diminishing contribution of diseases to deaths on the battlefield is ever present —since World War I, deaths from naturally occurring infections have not exceeded deaths due to combat injury in wartime. Global health and human diseases caused by Mother Nature do not immediately conjure the same concerns. Global health threats have been associated more closely with natural disasters, disaster assistance, and humanitarian operations; but there is much more to it than that. In our increasingly interconnected world, global health cannot be separated from global and national security.

Our modern world has allowed—and even encouraged—people to travel across borders, from country to country, and even from continent to continent. With an ever-increasing global economy we import/export goods with greater ease than ever before. Be it by ship, plane, or high-speed rail, people and goods are able to move more freely. The same ease of transport applies to the spread of infectious disease—bacteria, viruses, and other pathogens do not recognize borders and have no need for passports. What they do need is 'carriers' or 'spreaders' of disease; the disease transmitters do not even need to be sick (asymptomatic)—they are just convenient 'vectors.'

This is not a new concept; diseases have been spread inadvertently across seas for a long time. Consider the Bubonic Plague, or the Black Death, which ravaged much of Europe from 1346-1353. The epidemic is thought to have spread mostly through infected fleas aboard ships traveling from country to country. Many hypothesize the disease originated from central Asia, and only spread because of the transportation between countries.[1] The potential for transmission of infectious disease has simply been amplified by the number of planes, trains, and ships that connect countries with higher frequency and greater speed.

In recent years, severe acute respiratory syndrome (SARS), West Nile Virus (WNV), Pandemic Flu (H1N1), avian or bird flu (H5N1), and HIV/AIDS have all spread across countries and continents due to the ease of travel.

A businessman unknowingly spread SARS after contracting the disease in his home country and then traveling to Hong Kong where ten others contracted the illness. These ten travelers rapidly spread the ill-

(Continued on Page 7)

[1] Benedictow, Ole, "The Black Death: The Greatest Catastrophe Ever," *History Today* 55, no. 3 (2005), accessed July 29, 2013, http://www.historytoday.com/ole-j-benedictow/black-death-greatest-catastrophe-ever.

*Image courtesy of artur84/FreeDigitalPhotos.net.

(Continued from Page 6)

ness across the globe to other parts of Asia, Europe, and North America. This resulted in 774 deaths in 29 different countries.[2]

WNV was once unknown to Americans. Tropical regions of Africa, southern Asia, and parts of Australia were the main areas where this disease was endemic. However, in time, whether it was an infected traveler, or mosquitoes trapped in plane cargo space or transported in another way, the disease made its way to the United States. WNV has a very low fatality rate, and most infected people are asymptomatic.[3]

H1N1, a 2009 strain of influenza, found its way around the world after a localized outbreak in Mexico was spread by returning travelers to persons who then initiated disease clusters across the globe. In less than two months, the virus had spread to dozens of countries creating a pandemic.[4] This was only possible because of the ease of global travel.

Also, consider HIV/AIDS. In the early 1970s, U.S. citizens did not consider it possible to contract such a disease. Yet in just 1982 the first of many congressional hearings was convened to address its spread in the United States, with the Centers for Disease Control (CDC) estimating that tens of thousands were already affected by the disease.[5] Though many questions revolve around the virus's origin, it had no trouble making its way around the world to become a global concern.

Without a passport and with disregard for country borders, infectious agents can and will spread freely. As the world becomes more connected, it has been recognized that global health is a security concern. The enemy is not tangible, but it is real and unpredictable. Therefore, government agencies need to recognize and be prepared for the potential of a global health disaster.

Preventative measures are in place to help control the spread of diseases from other countries. People planning to visit certain regions of the world have mandatory vaccinations prior to their trip. Additionally, those applying for an immigrant visa and refugees must undergo a medical examination to determine if they can safely be admitted into the United States.[6] However, even with these preventative measures the United States remains vulnerable. There are risks for new, fatal, infectious agents to be introduced to the country at anytime thanks to global transportation networks.

The CDC places a strong emphasis on preparedness in the wake of an emergency. To protect the United States, the CDC conducts research, surveillance, and works with the government to implement necessary plans and policy in the wake of a health disaster.[7] The CDC also recognizes the correlation between travel and he potential spread of disease. It provides resources to best prevent infectious agents from joining travelers on their journeys.

Additionally, the U.S. Department of Homeland Security (DHS) recognizes that part of its mission to secure the country from both manmade and natural disasters includes the threat of widespread health emergencies. Within DHS, the Office of Health Affairs devotes energy to Health Threat Resilience so that it can better "respond to catastrophic health threats."[9]

In 2005, Woolhouse and Gowtage-

(Continued on Page 8)

---

[2] Ostroff., Stephen M. "Introduction: Perspectives: The Role of the Traveler in Translocation of Disease." In *CDC health information for international travel 2014: the yellow book.* Oxford University Press, 2013, accessed July 31, 2013, http://wwwnc.cdc.gov/travel/yellowbook/2014/chapter-1-introduction/perspectives-the-role-of-the-traveler-in-translocation-of-disease.

[3] Kilpatrick, A. M.. "Globalization, Land Use, And The Invasion Of West Nile Virus." *Science* 334, no. 6054 (2011): 323-327.

[4] Ostroff, "Introduction: Perspectives: The Role of the Traveler in Translocation of Disease."

[5] A Timeline of AIDS: 1982. http://aids.gov/hiv-aids-basics/hiv-aids-101/aids-timeline/.

[6] "Medical Examination of Immigrants and Refugees". Centers for Disease Control and Prevention, accessed March 29, 2012, http://www.cdc.gov/immigrantrefugeehealth/exams/medical-examination.html.

[7] "A New Era of Preparedness," Centers for Disease Control and Prevention, March 27, 2008, http://www.cdc.gov/CDCTV/EraOfPreparedness/index.html.

[8] Ostroff, "Introduction: Perspectives: The Role of the Traveler in Translocation of Disease."

[9] "Office of Health Affairs," U.S. Department of Homeland Security, http://www.dhs.gov/office-health-affairs.

(*Continued from Page 7)*

Sequeria[10] surveyed the literature concerning emerging and reemerging pathogens. They identified 1,407 recognized species of human pathogen. Of that total, 177 are regarded as emerging or reemerging. Interestingly, they further identified that the main categories of 'drivers' associated with those diseases affecting humans were almost all associated with changes in human behavior. The data is presented below.

Rank*	Driver(s)
1	Changes in land use/ agricultural practices
2	Changes in human demographics & society
3	Poor population health
4	Hospitals & medical procedures
5	Pathogen evolution
6	Contamination of food or water sources
7	International travel
8	Failure of public health programs
9	International trade
10	Climate change

**Ranked by the number of pathogen species associated with the item.*

How many of those behaviors will continue to change in favor of the pathogens over the coming decades? Very few can be reversed. One of the most 'hotly' debated topics over which we may exert some influence—climate change—ranks only tenth; how will that change in the coming years? William H. Foege, the former CDC Director (1977-1983) wrote that "People are beginning to understand there is nothing in the world so remote that it can't impact you as a person." With all those bugs on the move, you can run but you cannot hide—"never mind the salt—pass me the antibiotics." ❖

[10] Woolhouse, M.E.J., & Gowtahge-Sequeria, S., "Host Range and Emerging and Reemerging Pathogens." *Emerging Infectious Diseases* (2005), Vol.11, No. 12, 1842-1847.

Risky Business: Will Reduced Biosecurity Funding Compromise U.S. Healthcare Sector Critical Infrastructure Security and Resilience?

by Jassandra Nanini, J.D., CIP/HS Research Associate

Immediately following the September 11, 2001 terrorist attacks, letters contaminated with anthrax spores were sent to numerous media outlets and two U.S. Senators. Exposure to the spores infected 22 people and resulted in five deaths, constituting the worst biological attack in U.S. history. Known by the FBI file name "Amerithrax," the resulting investigation was among the "largest and most complex in the history of law enforcement."[1]

The robust Seven-Year Amerithrax Task Force expended over 600,000 investigator work hours and involved, among others, 25-30 full-time FBI investigators, the U.S. Postal Investigation Service, and federal prosecutors.[2] Their efforts included more than 10,000 witness interviews spanning six continents, 80 search executions, and over 6,000 items of potential evidence. The grand jury issued more than 5,750 grand jury subpoenas.[3] Investigators began with 31 million printed envelopes, 1.8 million postal items, 120,000 environmental samplings, and 17,000 suspect leads.[4] Researching the source of the anthrax strain involved 20 laboratories, 1,070 isolates with 8 morphotypes, and 4 genotypes.[5] In total, the investigation lasted 10 years and clean-up costs reportedly exceeded $1 billion.[6]

The immense effort and expense required to address this relatively small-scale attack involving only a handful of letters illustrates the potent danger posed by biological threats. The profoundly expansive investigation also highlighted the limited biodefense infrastructure at the time, as few labs had sufficient capacity and containment standards to process the voluminous samples. This new awareness led the National Institute of Allergy and Infectious Diseases (NIAID) to develop the Strategic Plan for Biodefense Research,[7] which outlined research and development objectives to address threats posed by potent pathogens and laid the foundation to create Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases (RCEs).[8]

Ten RCEs were established, with each consisting of a conglomerate of research institutions and universities serving a specific geographical region. Designed to "maintain a strong scientific infrastructure supporting multifaceted research and development activities that promote scientific discovery and translational research capacity required to create the next generation of therapeutics, vaccines, and diagnostics,"[9] a subset of these RCEs

(Continued on Page 10)

---

[1] "Famous Cases & Criminals: Amerithrax or Anthrax Investigation," *FBI*, last accessed August 12, 2013, http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax/amerithrax-investigation.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Allan Lengel, "Little Progress in FBI Probe of Anthrax Attacks," *Washington Post*, September 16, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/09/15/AR2005091502456_pf.html.
[7] "NIAID Unveils Biodefense Research Agenda," *NIH News*, March 14, 2002, http://www.niaid.nih.gov/news/newsreleases/2002/pages/biotagenda.aspx.
[8] "Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases (RCEs)," *National Institute of Allergy and Infectious Diseases (NIAID)*, last updated November 3, 2011, http://www.niaid.nih.gov/labsandresources/resources/rce/Pages/default.aspx.
[9] Ibid.

(Continued from Page 9)

house Regional Biocontainment Laboratories (RBLs) capable of handling dangerous pathogens such as anthrax.[10] Together, the RCEs and RBLs established a new, robust critical infrastructure capacity and capability in the Healthcare Sector, providing facilities, resources, skilled personnel, and new knowledge to respond to biological threats in post-9/11 America.

State and private funding have been insufficient to support the operations of the RCEs and RBLs, leaving federal financing as the raft to keep them afloat. In the past two years, however, a growing trend of defunding and re-prioritization threatens their fiscal security. The April 8, 2011 budget agreement designed to cut the federal spending and avoid a government shutdown[11] cut $300 million from the NIAID infectious disease research programs, $85 million from state and local public health preparedness programs, and $60 million from the Hospital Preparedness Program grants.[12] This commenced a trend in budgetary reductions for bio-defense, culminating in 2014 with the cessation of direct federal funding for the RCEs, which will instead have to apply for grants, resulting in reduced money for the RBLs as well.

The ramifications of federal defunding could prove to be multifaceted. The shift in budgetary allocations indicates a corresponding reordering of priorities related to critical infrastructure security and resilience, as the federal government invested billions in biodefense programs after 9/11, but now appears unwilling to maintain the fruits of that investment. Presumably, the threat of a viral or bacterial outbreak no longer appeared to justify the substantial cost of ensuring the program's fiscal security. Outside the short-lived anthrax scare and small-scale cases of ricin poisoning and monkeypox, the United States has primarily faced threats from large-scale outbreaks of H1N1 and SARS. The difficulty in weaponizing biological agents has assuaged fears that the next major terrorist attack will target health instead of physical infrastructure. These factors have generated a perception of relative stability in the domestic health system.

This sense of security, however, may be dangerously misplaced. On the terrorist front, deadly and highly contagious agents still exist around the world, and the technology of weaponization is ever-advancing. For one, smallpox samples reportedly went missing from the U.S.S.R. in the 1980s and have not been recovered to date. Despite the fact that smallpox is supposedly kept only at the Centers for Disease Control (CDC) in Atlanta and in Russia's Vector Laboratory, some believe that North Korea also has its own stores, obtained from Russian scientists. There are also suspicions that al Qaeda has sought a source for samples to weaponize.

Anthrax continues to pose a threat, as the registered list of facilities with anthrax stocks was founded on an initial, voluntary baseline. Updates to the baseline are mandatory, but sites with historical anthrax stocks—some unwitting—remain a potential concern. After the initial anthrax mailings, when the FBI was asked how many labs in the United States had anthrax spores, no one knew. Records existed for documented transfers, but many transfers were undocumented, and no records had been kept of where anthrax studies were previously conducted. There is no way to determine where unreported samples may be today.

Even more alarming, the cost of replicating viruses has dropped dramatically.[13] The cost of determining one megabase of DNA sequence has fallen to less than a

(Continued on Page 11)

---

[10] "US BSL Laboratories," Federation of American Scientists, accessed August 12, 2013, http://www.niaid.nih.gov/news/newsreleases/2002/pages/biotagenda.aspx.

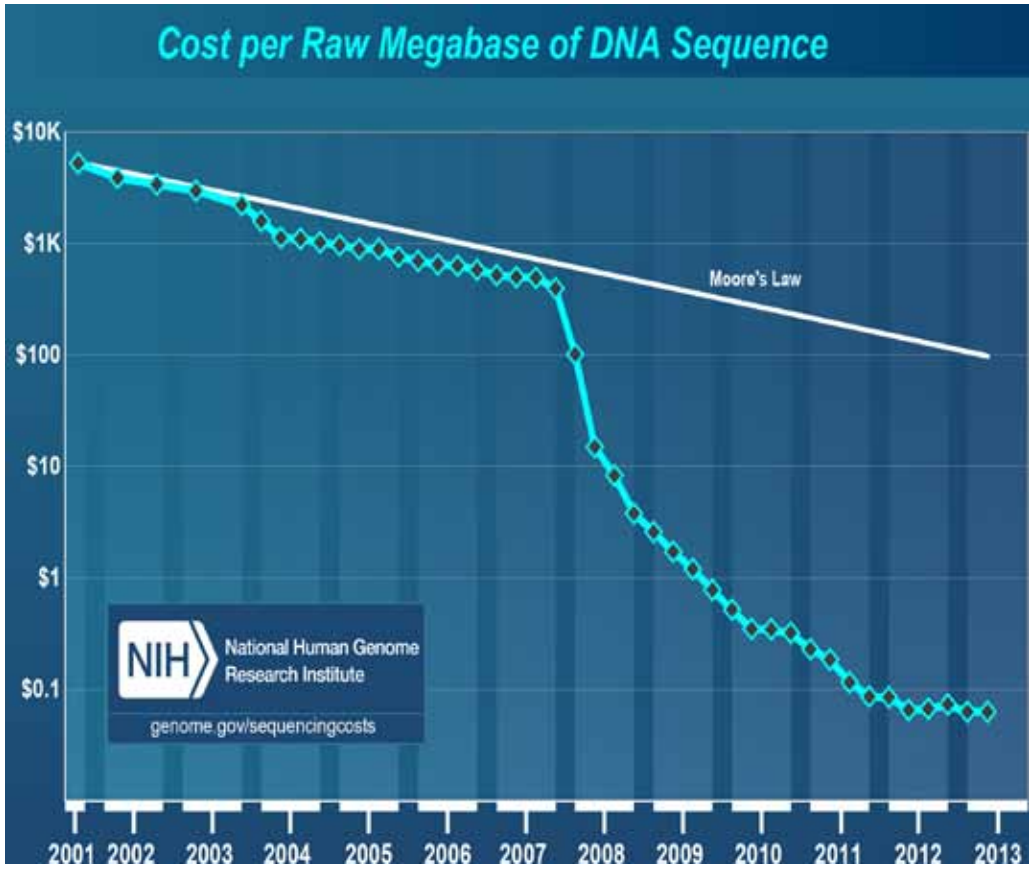
[11] Carl Huse, "Budget Deal to Cut $38 Billion Averts Shutdown" *New York Times*, April 8, 2011, http://www.nytimes.com/2011/04/09/us/politics/09fiscal.html?pagewanted=all&_r=0.

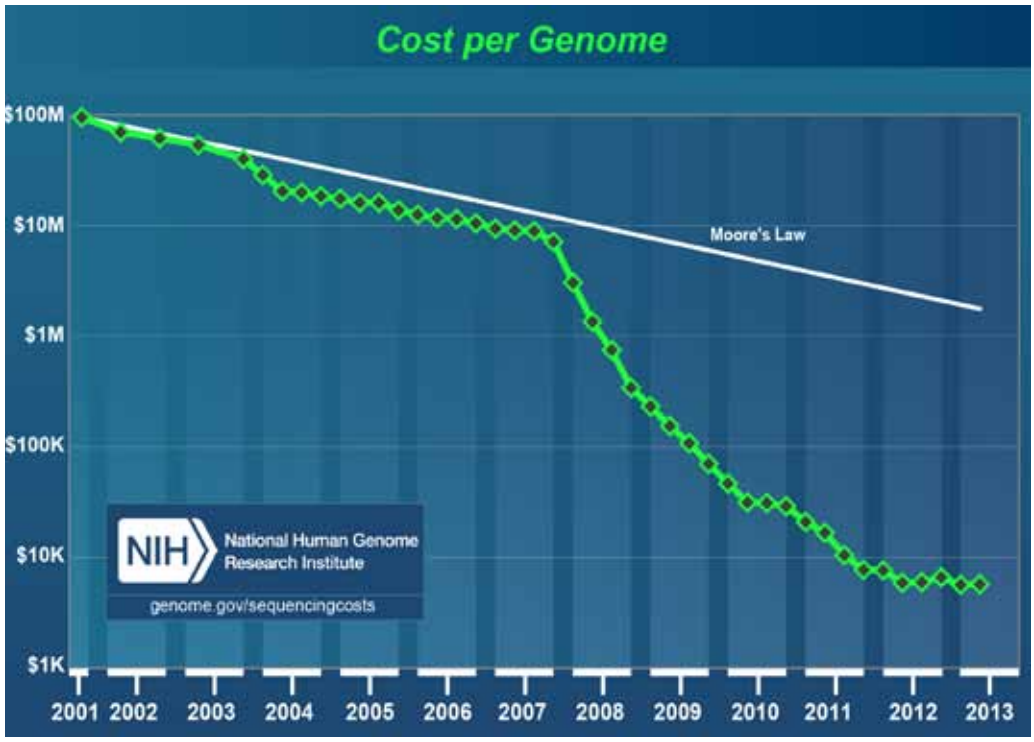
[12] Alex Phillippidis, "A Decade after 9/11, Spending Cuts Challenge Biodefense Effort Spawned by Attacks," *Insight & Intelligence: Genetic Engineering & Biotechnology News*, September 11, 2011, http://www.genengnews.com/keywordsandtools/print/3/24305/. For detailed information on biodefense budget allocations and trends through Fiscal Year 2012-2013, see Crystal Franco and Tara Kirk Sell, "Federal Agency Biodefense Funding, FY 2012-2013," *UPMC Center for Health Security*, November 2, 2012, http://www.upmchealthsecurity.org/website/resources/publications/2012/2012-06-12-biodeffunds.html.

[13] "DNA Sequencing Costs," National Human Genome Research Institute, updated July 16, 2013, http://www.genome.gov/sequencingcosts/.

(Continued from Page 10)

dollar, while the cost of synthesizing a single human-sized genome has dropped to around $8,000. This is down from approximately $7,500 per megabase of sequencing and $100 million per genome in 2001.[14] These figures indicate that for under $10,000 a terrorist could isolate and replicate a malicious virus in his own garage using equipment purchased online. With the plethora of information available online and the automation of modern equipment, limited skill is required. Long gone are the times that biological warfare required state sponsorship, or even access to a sophisticated lab facility.





The capability also exists to create a virus from scratch, without a sample, as long as the sequence is already available. In 2002, when synthesis was prohibitively more expensive, the Department of Defense funded the creation of a live polio virus from chemicals and genetic information readily available to the public.[15] This implication is alarming in the face of the rapid technological advancements of the last decade.

(Continued on Page 12)

[14] Ibid. For further discussion of the costs and capabilities of modern DNA sequencing and synthesis, see Robert Carlson, "The changing economics of DNA synthesis," Nature Biology 27, no. 12 (December 2009): 1091-1094; Robert Carlson, "New Cost Curves," *Synthetic Biology*, June 17, 2011, http://www.synthesis.cc/2011/06/new-cost-curves.html.

[15] Andrew Pollack, "Traces of Terror: The Science; Scientists Create a Live Polio Virus," *New York Times*, July 12, 2002, http://www.nytimes.com/2002/07/12/us/traces-of-terror-the-science-scientists-create-a-live-polio-virus.html?pagewanted=all&src=pm.

(Continued from Page 11)

Threats exist outside the scope of terrorist activity as well. Naturally occurring diseases are continuing to emerge. The cost of containing an outbreak of even a non-deadly disease could bankrupt states without sufficient federal support. Biomedical research to improve identification, treatment, and containment of such diseases is critical to creating resilience in the Healthcare Sector.

This begs the questions of whether the RCEs and RBLs will survive without federal support, and if they do not, where will it leave U.S. biosecurity, biosafety, and bio-containment? The problem begins with a vacuum of relevant research. The more effort scientists in these centers devote to knowledge about biological threats and mitigation of the potential harms, the more effective and timely the response to a threat or outbreak.

Moreover, a widespread outbreak would require the testing and support resources of more than just the CDC—regional centers enable a coordinated and immediate response throughout the nation and provide a necessary surge capacity. Samples would more readily be tested, experts would be available to educate health care providers, and real-time research to address the outbreak would be widespread and robust. Without the centers, the CDC would bear the primary burden of setting up response teams in each state, assigning experts, and researching the scientific nature of the disease. In other words, the 'critical' infrastructure that already exists would need to be refashioned in the midst of an emergency.

Additionally, if shut down, the RBLs may fall out of repair, be diverted to other uses, or be completely abandoned. This would not only constitute a gross waste of resources, but also leave countless biodefense scientists out of work. If there is no market in the United States, they will need to retrain in other specialties, or may seek employment abroad.

Finally, decreased funding of biosecurity increases the total risk of a biological attack. Risk comprises the multiplication of threat, vulnerability, and consequence. Physical infrastructure has been a favorite terrorist target because of the potential for high loss of life. However, increases in surveillance and airport security, along with a recent string of failed attack plans, have made this tactic more costly and less effective. Yet, the cost of developing deadly biological agents has dramatically decreased, just as educational resources and equipment have become easily accessible online. Decreased cost and increased availability equates to increased threat. Instead of reducing vulnerability in response to this increased threat, reduced funding for RCEs, and consequently RBLs, jeopardizes the extensive critical infrastructure implemented precisely to thwart this growing danger, leaving the United States more vulnerable, and increasing the risk of a potentially devastating biological outbreak.

Some commentators have likened laboratory critical infrastructure to an insurance policy against the rising risks from biological threats. Extending that analogy, the time to cancel the policy or reduce coverage is not just prior to an accident, or when circumstances make an accident more likely. We cannot predict precisely when we will next need our critical facilities any more than we can predict when we might be involved in an accident. Decreased funding for these critical facilities is equivalent to purchasing cut-rate insurance—we may enjoy the savings now, but will we regret it later? ❖

Critical Infrastructure Protection and Global Health

by Elvira Beracochea, M.D., M.P.H.*

The Global Problem of CIP and Health

With the exception of the United States, Australia, and some European countries, critical health infrastructure protection (CHIP) is a new field within healthcare. CHIP is essential, though, to ensure the continuous provision of quality health care to human beings. Preparedness for incidents that affect the health and care of large population groups is limited to the organized response to rapidly serve the victims of natural or manmade disasters, and prevent further harm to others. Protection of critical healthcare infrastructure is not part of the first response effort, which is instead responsible for protecting human life during emergencies. In addition, infrastructure protection is limited to protecting a country's own assets and does not address the impact of risks and potential incidents on global infrastructure. Consequently, there is not a global CHIP plan focused on identifying risks and protecting infrastructure that is critical to global health stability.

As with any new field of study there are ongoing dialogues about what should and should not be included in CHIP. The Tasmanian (Australian) Emergency Management Plan[1] suggests that "Once identified, a list of critical health infrastructure and their key interdependencies should be maintained and all existing security, on-site emergency and business continuity management plans should be reviewed." Arrangements for the protection of the identified critical health infrastructure should be included in 'Area Health Service' emergency management plans and relevant supporting plans and include:

a. Providing adequate security for identified assets.
b. Actively applying risk manage ment principles to planning processes.
c. Regularly reviewing risk management assessments and plans.
d. Reporting any incidents or suspicious activities.
e. Regularly reviewing business continuity management plans.
f. Participating in exercises that test and validate arrangements.

This approach is consistent with that promoted by the U.S. Department of Homeland Security for critical infrastructure security and resilience and could provide an effective basis for discussions and implementation of international efforts to establish CHIP.

At national and sub-national levels, tangible and intangible health infrastructure assets exist that require identification, maintenance, and protection. Tangible assets include a nation's health workforce; facilities such as clinics, hospitals, and storage units; medicine inventories; equipment; ambulances and other vehicles; public health management bodies; and educational institutions such as medical and nursing. Intangible assets include patient medical records, epidemiological surveillance, and health management information. Most developing countries do not have up-to-date records identifying facilities and health-related buildings, and such facilities often do not have inventories of their equipment or plans for its replacement in the event of sudden destruction due to local violence, acts of war, or natural disasters. Moreover, these countries do not have sufficient funds or staff

(Continued on Page 14)

[1] Department of Health and Human Services Emergency Management Plan, Tasmania, June, 2011.

(Continued from Page 13)

who understand the preparedness actions required to protect and/or replace their clinics, hospitals, or medical and nursing schools should they be destroyed by natural or man-made disasters.

The Road Ahead

What follows is a simple roadmap to begin the journey to global health critical infrastructure protection that would ensure the continuity of health services to the populations directly affected by natural or man-made disasters.

1. An effort should be made to identify a repository of information relevant to critical health infrastructure by country. WHO would be the repository of choice by building on its health observation technology and network of country offices worldwide.

2. Ensuring continuous and sustainable healthcare requires understanding of the capabilities and maintenance requirements for physical healthcare infrastructure. This begins with dissemination of instructions for each country to identify its critical infrastructure. For example, Malawi has at least one district hospital and a number of health centers in each of its 29 districts. In addition, the Christian Health Association of Malawi (CHAM) manages a number of hospitals, health centers, and nursing schools. All of these government and CHAM facilities, some built with donor funding from organizations such as the United Nations High Commissioner for Refugees (UNHCR), are critical to protect the lives of Malawians and refugees from neighboring countries. A need exists for such an inventory, along with a plan to maintain these facilities so they may continue providing health services according to quality standards.

3. After countries identify their critical health infrastructure, they must identify risks affecting that infrastructure and develop plans for prevention and mitigation of harm in the event of an incident. The relevant national health department must be primarily responsible for planning and monitoring implementation of their maintenance and protection plans. As is the case with Malawi, the funding and implementation must be coordinated with all stakeholders in each respective district.

4. Health infrastructure belongs to all and everyone retains the responsibility to protect it. Every health facility must have a CHIP plan and someone should be responsible for ensuring that health providers and community members are prepared. This involves making sure community leaders and local authorities are aware of the importance of preserving the health infrastructure for present and future generations. In Malawi, for example, village chiefs must be empowered to realize that health centers are critical infrastructures that belong to them and ensure continuity of care to their villages. Village chiefs can educate their communities regarding the value of a facility and the cost of replacing it, and encourage villagers to participate in regular painting, cleaning, and minor repair of their "own" critical infrastructure.

5. Advancements in CHIP reporting are also necessary. Countries must be able to report on the current status of their critical health infrastructure to identify and strategically address global gaps. WHO must acknowledge accountability for existing critical health infrastructure, starting with physical facilities, and this effort requires support from donor agencies and assistance organizations.

6. Critical infrastructure health research must be expanded to identify cost-effective ways for its protection in every country. Action research to develop templates for CHIP need to be carried out. We must not take health infrastructure for granted and should make efforts to ensure this mentality is globalized.

The current status and future of CHIP remains unknown. Preparedness would help prevent infrastructure losses, strategically plan its growth and development, and save lives. CHIP is not just a matter of homeland security, but of responsible stewardship of the collective health assets of present and future generations worldwide.❖

**Dr. Beracochea is the founder, president, and CEO of MIDEGO, Inc., a global health workforce development and system strengthening firm committed to achieving the Millennium Development Goals. She is also an adjunct professor at George Mason University and can be reached at elvira@midego.com.*

Increasing Hospital Resilience

by Anna Bethke, Dave Brannegan, and Kelly Wallace,
Infrastructure Assurance Center, Decision and Information Sciences Division,
Argonne National Laboratory

Introduction

A community relies on its hospitals to provide general medical care (e.g., outpatient, clinical, and surgery services) and emergency medical services 24 hours a day, 365 days a year. Natural hazards, such as earthquakes, floods, tornados, and hurricanes, can greatly impact a hospital's ability to provide necessary care to a community during times of severe need. As a result, it is critical that hospitals analyze, understand, and improve their resilience—the ability to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance.[1] In particular, hospitals can enhance resilience, thereby reducing the impact of disruptions, by addressing operational dependencies, strengthening resilience planning efforts, and implementing short- and long-term physical design resilience measures.

The Infrastructure Assurance Center (IAC) at Argonne National Laboratory, in partnership with the Protective Security Coordination Division of the U.S. Department of Homeland Security (DHS), developed the Resilience Measurement Index (RMI) to characterize the resilience of critical infrastructure assets.[2] The RMI data is collected during facility surveys conducted as part of the DHS Enhanced Critical Infrastructure Protection (ECIP) program.[3] The following gives an overview of the current resilience characteristics of hospitals participating in the ECIP program nationwide in order to illustrate the key resilience-related efforts being undertaken by these facilities. Common improvements in resilience, as deduced from these characteristics, are also presented. The IAC analyzed data from 165 hospital surveys conducted between January 2011 and July 2013.

Operational Dependencies

In general, hospitals depend upon external sources for electric power, natural gas, water, wastewater discharge, communications, information technology services, and critical products (e.g., oxygen, blood, and other medical supplies) to maintain core operations. Loss of any one of these services can severely degrade facility operations. However, the ECIP survey data shows that most hospitals have an alternative source or backup to mitigate the impacts from the loss of most of these dependencies. The operational capacity and duration of these backups greatly impact how well a hospital is able to continue to provide their full range of services after a failure or disruption occurs. For instance, nurses at New York University Langone Medical Center had to hand-squeeze oxygen bags for patients after the hospital's electric generator unexpectedly failed at the height of Hurricane Sandy.[4] Of the hospitals surveyed, most have backup capabilities to sustain core operations for 1-2 days after

(Continued on Page 16)

[1] Carlson, J. L., R. A. Haffenden, G. W. Bassett, W. A. Buehring, M. J. Collins III, S. M. Folga, F. D. Petit, J. A. Phillips, D. R. Verner, and R. G. Whitfield. *Resilience: Theory and Application*. No. ANL/DIS-12-1. Argonne National Laboratory (ANL), 2012.
[2] Petit, F. D. P., G. W. Bassett, R. Black, W. A. Buehring, M. J. Collins, D. C. Dickinson, R. E. Fisher, R.A. Haffenden, A.A. Huttenga, M.S. Klett, J.A. Phillips, M. Thomas, S.N. Veselka, K.E. Wallace, R.G. Whitfield, and J.P. Peerenboom *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*. No. ANL/DIS-13-01. Argonne National Laboratory (ANL), 2013.
[3] Ibid.
[4] Italie, Leanne and Marchinoe, Marilynn. Associated Press. "NYU Hospital Evacuation: Hurricane Sandy Power Failer Moves More than 200 Patients." http://www.huffingtonpost.com/2012/10/30/nyu-hospital-evacuation-hurricane-sandy_n_2044026.html. Accessed Aug. 6, 2013.

(Continued from Page 15)

their primary source failed or was disrupted, albeit at a reduced operational capacity. Figure 1 illustrates how a typical hospital could be affected by the loss of each dependency over a 3-day time span.[5] This figure displays the percentage of degradation to core operations over time. Depending upon the service, the facility may experience an immediate impact to operations (e.g., loss of electric power), or operations may not be impacted for several hours (e.g., loss of natural gas). After a service loss, available backups will be utilized to support either full core operations or select operations (e.g., safe shut-down) as shown by the percentage of degradation or impact. Once the backup fails (e.g., fuel for emergency generators runs out), there is typically a further degradation of operations. Finally, once the service is restored, there may be a delay until the facility can begin to operate at full capacity again.

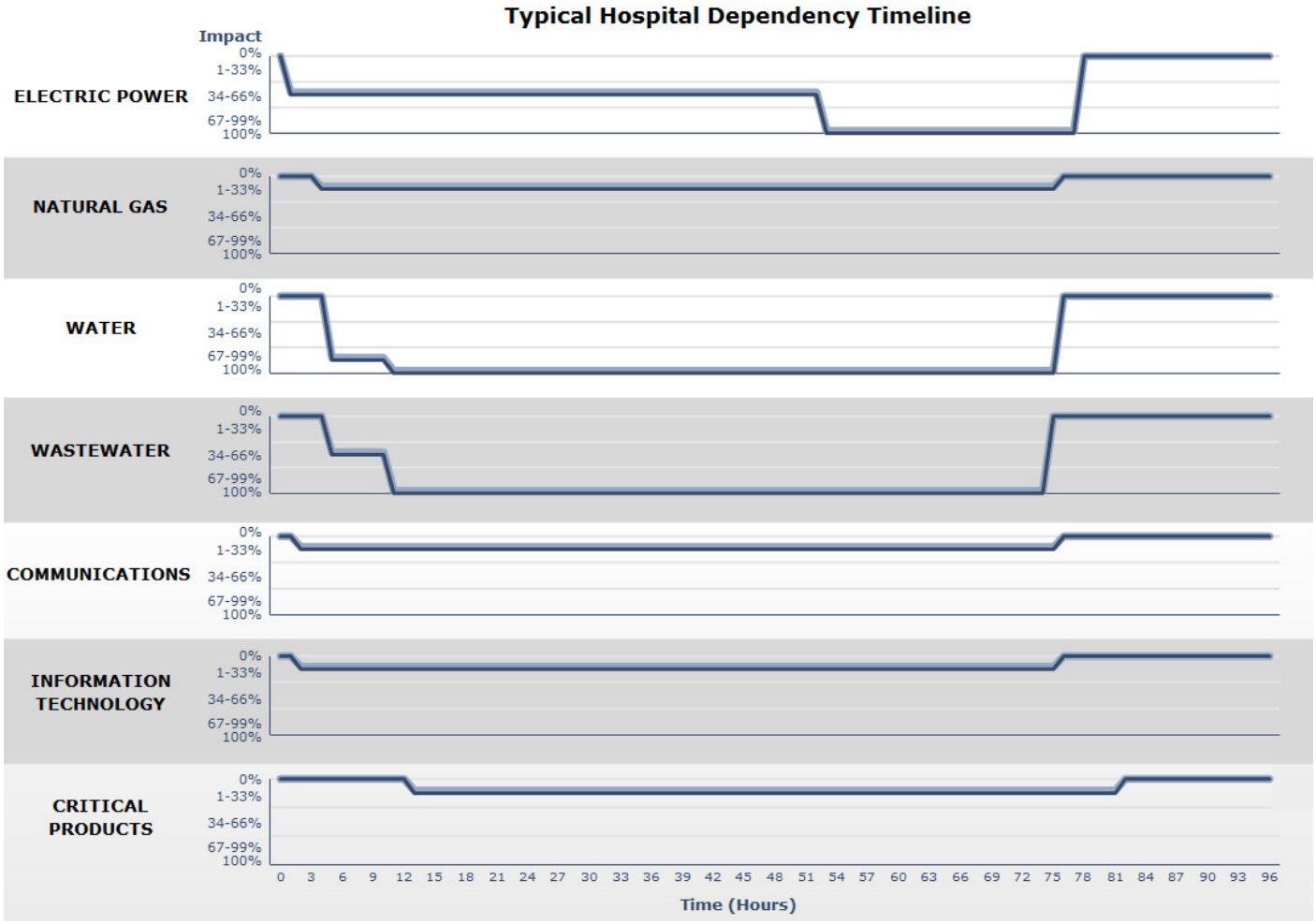


Figure 1: A Typical Hospital's Dependency Impact Over Time

By improving the operational capacity and duration of a facility's backups, dependency-related impacts can be reduced. For instance, one backup generator may use diesel fuel and require daily refueling but can provide electric power for 75 percent of the facility's load. A different backup generator may operate via a direct fuel source (e.g., natural gas) that would permit the generator to run continuously; however, it may only provide enough electric power for 50 percent of the facility's load. Figure 2 illustrates the effect these two scenarios have on how long and how much a hospital would be impacted by a power loss.

(Continued on Page 17)

[5] Three days is the timeframe for this illustrative display because it corresponds to the Federal Emergency Management Agency (FEMA)-recommended preparedness duration for the general population and organizations in the event of an emergency resulting in the breakdown of major services. FEMA. *FEMA Strategic Plan* (February 2011) http://www.fema.gov/pdf/about/strategic_plan11.pdf. Accessed August 1, 2013.

(Continued from Page 16)

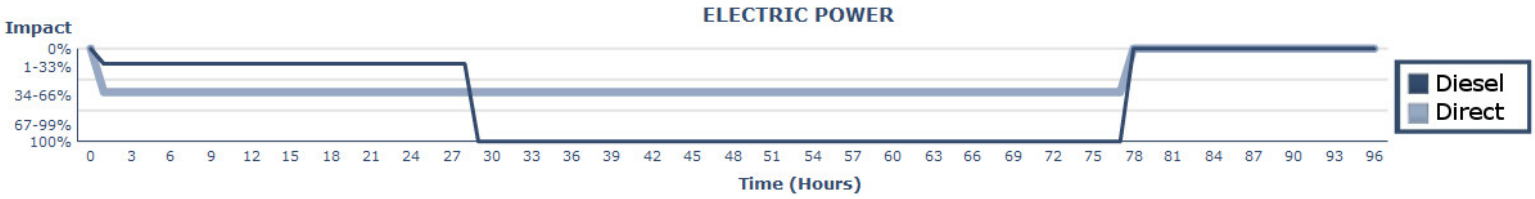


Figure 2: Comparison of Two Electrical Backup Generators

By improving the operational capacity and duration of a facility's backups, dependency-related impacts can be reduced. For instance, one backup generator may use diesel fuel and require daily refueling but can provide electric power for 75 percent of the facility's load. A different backup generator may operate via a direct fuel source (e.g., natural gas) that would permit the generator to run continuously; however, it may only provide enough electric power for 50 percent of the facility's load. Figure 2 illustrates the effect these two scenarios have on how long and how much a hospital would be impacted by a power loss.

Overall, hospitals are reasonably equipped with sufficient backup of operational dependency sources to ensure continued operations, but improvements can be made, particularly in the water and wastewater backups. The longer a hospital has access to the supplies and operational dependencies it requires, the longer it will be able to provide its primary function—the care of its patients.

Resilience Planning

Comprehensive resilience planning includes, but is not limited to, formally creating, exercising, and providing training on business continuity plans and emergency operations or emergency action plans. In addition to these plans, establishing an incident management and command center (IMCC) can help the facility coordinate response and recovery efforts in an emergency.

Establishing comprehensive plans and procedures for business continuity can allow hospitals to better maintain or recover their normal business operations in the event of a disruption. Of the hospitals surveyed, 75 percent have established business continuity plans. Most of these plans included alerting employees, notifying suppliers and utility providers, and identifying key emergency personnel by position. The majority of the hospitals with business continuity plans trains their employees on the provisions of the plan and exercise it at least once a year.

An emergency operations or emergency action plan can establish a hospital's overall incident strategy, tactics, risk management, and member safety.[6] Ninety-nine percent of the hospitals surveyed have emergency action plans. These plans typically included evacuation routes, up-to-date rosters for key personnel, as well as procedures for extended utility loss. Nearly all facilities trained employees on the provisions of the plan and exercised the plan at least once a year. In case of an emergency, 96 percent of the hospitals surveyed have an IMCC from which the facility can manage emergency operations, but only 60 percent of these IMCCs can operate independently of all external utilities for at least three days.

On average, the current resilience planning of those hospitals surveyed is comprehensive; however, continual review and improvement of these plans is necessary to account for changing assets and hazards.

Resilience of Physical Design

Mitigating construction, modifications, or retrofitting can reduce the impacts from relevant natural hazards, as can implementing short- and long-term mitigation measures specific to an approaching hazard. In 2007, the Federal Emergency Management Agency (FEMA) released a hospital building design guide to reduce the impact of natural hazards.[7] However, only 30 percent of

(Continued on Page 18)

[6] NFPA (National Fire Protection Association). *NFPA 1600-Standard on Disaster/Emergency Management and Business Continuity Programs-2010 Edition*. Quincy, MA: NFPA, 2010.
[7] FEMA (Federal Emergency Management Agency). "Design Guide for Improving Hospital Safety in Earthquakes, Floods, and High Winds." (2007). http://www.fema.gov/media-library/assets/documents/10672?id=2739. Accessed July 30, 2013.

(Continued from Page 17)

the hospitals surveyed were constructed, modified, or retrofitted to withstand the natural hazards they typically experience. The FEMA report identifies permanent building considerations such as structural strengthening, lightning rods, and ensuring that essential facility components are raised above the 100-year floodplain.[8] Sixty percent of the hospitals surveyed have specific plans or procedures for long-term and immediate mitigation measures including preparing or deploying necessary equipment such as sandbags, temporary snow fences, or temporary sump pumps. These measures also include designating appropriate shelters for tornados or other severe weather hazards. Only 25 percent of the hospitals have deployable mitigation measures that include temporarily moving critical equipment, pre-emptively shutting down non-necessary equipment, or planning evacuations to an alternative location.

Based on the ECIP survey data, most hospitals have not pursued many resilience efforts with regard to their physical design. Doing so could improve how well the facilities are able to recover from natural hazards.

Conclusion

Hospitals must be resilient to a variety of hazards in order to continue providing care to the communities they serve. The resilience data collected via the ECIP survey shows that most hospitals have developed adequate dependency backups as well as established comprehensive resilience planning, but have not implemented many physical design mitigation measures. Depending upon the hazards they face, current mitigation measures, and existing resources, there are many options a hospital can pursue to improve their overall resilience. The data from the ECIP survey can be used to assess which resilience efforts are currently in place, and which should be further investigated to ensure that hospital patients have the best opportunity for continued medical services, regardless of what event may arise. ❖

[8] Ibid.