Government Business Council

When Someday Is Today

Lessons for Health Security and Disaster Mitigation

Underwritten by

CADMUS

After a succession of natural disasters across the country, the public is turning to preparedness directors and healthcare preparedness staff for aid and guidance. These professionals face numerous challenges in their mission to keep citizens safe: disease outbreaks, gaps in emergency health informatics, and the continued possibility of bioterror attacks on American soil.

To better understand how first responders in government are working to address these challenges, Government Business Council (GBC) conducted interviews with senior emergency preparedness leaders between August and September 2017. We asked them to describe what they see as the top threats to citizen safety, priorities for improving emergency response, and the importance of strategy, communication, and technology in preserving human lives.

Comprehensive Disease Response in the Information Age

Jeff Bryant, Director for the Emergency Operations (EO) division with the Centers for Disease Control and Prevention (CDC), oversees health security and emergency preparedness. Among his concerns is the environmental health damage that disasters unleash: "With flooded areas, there are often industrial contaminants that weren't there before, [so we help] the state think through how to mitigate that contamination and make sure the water treatment systems are back online."

Bryant raises communications frustrations that are echoed by the state-level experts interviewed for this report. He says "it's critical that the federal government [and states] speak with one voice. We've been working with our state partners in Texas and Louisiana to [standardize] the public health messaging around floodwaters, safe food [and] water precautions, and protection from insect and snake bites."

He also outlines the unique challenges associated with responding to manmade and natural disease threats: "With an infectious disease outbreak, CDC has a very different role than we do in a natural disaster response. We are the operational leads during a large international infectious disease response because we have the experts to manage the response. Specifically, [we have] people that are familiar with working in international environments with CDC." Three main categories of action are central to Bryant's response protocol: epidemiological analysis of disease outbreak, laboratory tests and diagnostics, and medical countermeasures aimed at prevention and containment — the success of all three hinges on effective use of data and technology.

> ...it's critical that the federal government [and states] **speak with one voice.**
>
> — Jeff Bryant
> Director, Emergency Operations
> Centers for Disease Control and Prevention

"One of the primary emergency management roles that we play is information sharing," says Bryant. "What do [preparedness directors] need to make the best decision they can make? We

put all [the data] together and just call it 'data management', but it's information flow [and IT]. It's secure information sharing." This is why Bryant sees the next few years as an opportunity for removing silos from collaboration efforts. "A lot of our partners that are experts in a particular disease, they have their own information systems [so] making sense of data management between epidemiology, surveillance data and laboratory data, [and] environmental data is a big task."

Emergency mitigation has seen an ascendance of technology-related strategy and roles in recent years — FEMA has had a chief technology officer (CTO) for at least half a decade and has been leveraging social media, mobile applications, and even search and rescue robots as part of its natural disaster response.[1] The digital explosion has been especially pronounced in preparedness communications, post-Katrina: states like Florida and Louisiana have taken robust measures to enhance the tools that professionals use in extreme, fast-paced response situations.[2]

Elizabeth Van Nostrand — Assistant Professor at the University of Pittsburgh and Director of the Mid-Atlantic Regional Public Health Training Center — shares her experience advising policymakers on the value of technology in emergency response: "We developed a tool called FRED, which shows outbreaks of infectious diseases and the impact of vaccination uptake and herd immunities. [We take] data and [digest] it to give people usable information [using tools] like GIS. It's really important for emergency preparedness — being able to map things — to allocate resources appropriately or to prepare."[3] Van Nostrand's hope is that as responders see the power of visualizing outbreak scenarios in real time, the community at large will devote more funding and attention to life-saving informatics over time: "There has to be more money given to governmental public health to train them with respect to these informatics tools, so they can identify particularly vulnerable populations and the medically underserved."

Next-Generation Communication for Health Security

As Director of Emergency Preparedness and Operations with the New Jersey Department of Health (NJ DOH), Brendan McCluskey says leadership and communication are key to ensuring his team's responsiveness to state needs. "Leadership is the ability for me and my organization to influence what others do around the state." He adds that this leadership must extend to government and the private sector in order for NJ DOH to be "at the forefront of emergencies, both preparing for [them] and then operating, responding, and recovering from them."

[1] "The New Tech of Disaster Response, From Apps to Aqua-Drones", Wired Magazine. 2015. https://www.wired.com/2015/08/fema-disaster-tech/
[2] *Ibid.*

[3] "FRED Web", University of Pittsburgh Graduate School of Public Health. 2017. http://fred.publichealth.pitt.edu/

One key component of McCluskey's department's work is external communication. Though NJ DOH is working to enhance its ability to communicate with hospitals and other healthcare partners, McCluskey says there's no guarantee his information always reaches the appropriate health officials. "I might have information that's relevant to the medical professionals who work in emergency departments in hospitals. I don't have contact with every single one of them, but I might have contact with a group of individuals, and those individuals have a list of other contacts I need to reach. I'm never really sure whether or not the

Cadmus Perspective: Meeting the Challenge of Keeping Citizens Safe

Each year, we encounter new threats and disasters. Whether natural or man-made, cyber or physical in nature, these incidents share the same fundamental reality: Our response could have benefited from more preparedness planning and efforts to enhance resilience. More can always be done, and we will always be challenged to prove that doing more has been worthwhile, particularly when justifying past and future investments in preparedness and resilience.

That said, we can raise the bar in other ways by thinking in new directions. Budgets will always fluctuate; the goal needs to be to strive to do the most with the resources at hand.

The first step is to engage with a broader set of stakeholders from the beginning. Casting a wide net early gives organizations that may not have an obvious role to play the opportunity to identify their resources at the onset. Include regional, state, and federal representatives as well as the private sector. It is also important to engage community representatives, as they will be among the first responders to disasters.

Next, continue realistic training and exercises. Training and exercises should not be the goal, but the means by which we work to enhance preparedness and resilience. Train and exercise in a realistic manner and in ways that truly stress the system.

Finally, do not simply identify lessons learned—do something about them. Develop corrective action plans and aggressively work toward addressing those deficiencies, then start the cycle again. Update your plans and policies, conduct tests and exercises, and strive for continuous improvement.

The next natural disaster, terrorist attack, pandemic, or cyber attack could be tomorrow, next month, or next year. We cannot become complacent in, or delay, our preparedness efforts. There's no day like today to build upon all of the work done over the last few decades toward a stronger response.

Nitin Natarajan

Principal, Homeland Security Sector

Cadmus

CadmusGroup.com

messages that we send out actually get to that end user, and it only takes that one case where [the information] doesn't get to the person who needs it for there to be serious consequences."

Part of the difficulty, he says, stems from outdated informatics tools and IT that is poorly equipped to handle today's multitude of social networks and digital outlets.

"We have two systems we're currently using and both of them are homegrown, going back about 10 or 15 years. One system allows us to do situational awareness, incident management, and resource management. The other is our health alert network, which is designed to deliver important messages out to the people. Because these systems are homegrown, it's very difficult for us to keep up with the needs and changing software requirements, though we're now in the process of moving to a commercial solution to better reach our constituents."

According to McCluskey, such upgrades will help to bypass the organization's reliance on multiple lists of individuals. "Under this new solution, we don't need to rely on multiple different lists in our public health and healthcare professions to retransmit what we're sending to the appropriate individuals. The technology [allows us to] have people sign up directly for messages that we want them to have or that they want to have. We're [able] to communicate with them directly."

Among the concerns that McCluskey, Bryant, and other interviewees raise are the evolving threats to outdated health technology. In 2017, the Department of Health and Human Services (HHS) released a report about the widespread vulnerabilities afflicting state and local health IT systems. The team's finding culminated in an unequivocal call to action: "health care cybersecurity is a key public health concern that needs immediate and aggressive attention."[4]

The National Association of County & City Health Officials (NACCHO) reached the same diagnosis, finding health groups especially susceptible to cyber attacks for three reasons:[5]

1. Security for health information systems is not prioritized;
2. The high frequency of data exchange requires many open connections to a healthcare information system; and
3. The healthcare and public health workforce is largely untrained in cyber security practices.

And because healthcare records are now more likely to be stored digitally, these extremely sensitive data can be even more valuable than credit card information. With the rapid proliferation of medical devices and wearables in the Internet of Things (IoT), adversaries have more opportunities to steal or repurpose such devices for continued exploitation

[4] "Report on Improving Cybersecurity in the Health Care Industry", U.S. Department of Health and Human Services. June 2017. https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf

[5] Cybersecurity: Risks and Recommendations for Increasingly Connected Local Health Departments", National Association of County & City Health Officials. February 2015. https://www.naccho.org/uploads/downloadable-resources/Issue-brief-on-Cybersecurity-NA639PDF.pdf

of PII and other information.[6] The risk of leaving IT systems exposed is very clear, and there is certainly no shortage of illustrative examples: earlier this year, the National Health Service (NHS) breach caused significant disruptions in medical procedures and left thousands of patient records vulnerable.[7]

Despite the efficiencies these systems can bring, McCluskey is cognizant that technology isn't a cure-all and tempers his expectations of its benefits against his ultimate focus: ensuring the effective delivery of aid and resources. "If something like [Hurricane] Harvey hit here, if we had another Sandy or Katrina, or a massive pandemic influenza outbreak, it would be difficult for us to be able to adequately provide services to everybody who needs it. We are the ones that are responsible for the public," says McCluskey. "When the public loses faith in that responsibility and can't believe what we say, they're not going to listen to us when it's actually critical for them to listen to us."

> We are the ones that are **responsible for the public.**
>
> — Brendan McCluskey
> Director, Emergency Preparedness and Operations
> New Jersey Department of Health

Mitigating Disaster through Flexible Management

Dane Matthew is Director of the Office of Emergency Preparedness and Response (OEPR) with the Colorado Department of Public Health and Environment (CO DPHE). His primary responsibilities include coordinating federal grants related to emergency preparedness and collaborating with local entities to ensure statewide readiness for both natural and manmade emergency situations.

Matthew cites administrative burdens as a major frustration: "It has been a challenge to manage federal grant requirements, reporting processes, and administrative procedures while simultaneously working to improve support for our community partners." Despite these constraints, Matthew is enhancing Colorado's ability to mitigate damage from public health disasters, including the growth of statewide preparedness funding by more than $800,000 following a number of streamlining measures.

Nonetheless, Matthew says he is "100 percent confident" that Colorado is prepared for a variety of disaster scenarios — a confidence driven by his department's training operations, which includes activities like multi-regional coordination and the distribution of pharmaceuticals and other supplies to the public. Matthew has modified his state's response protocol and provides recommendations for other states' healthcare preparedness staff interested in ramping up their own. "Colorado modified [how] Hospital Preparedness Program funds are distributed to local communities. With the new mandate from [the federal government], funds are now directed

[6] "Medical Devices: Digital Health", U.S. Food and Drug Administration. September 2017. https://www.fda.gov/medicaldevices/digitalhealth/

[7] "NHS cyber-attack causing disruption one week after breach", The Guardian. May 2017. https://www.theguardian.com/society/2017/may/19/nhs-cyber-attack-ransomware-disruption-breach

to Health Care Coalitions to ensure a more robust planning and coordinating effort that involves hospitals, public health, and other healthcare organizations from around the state."

Multi-stakeholder response efforts can also be improved through the assumed participation of key partners in a practice known as 'opt-out default'. Studies show that simply permitting participation (i.e., using an 'opt-in' approach) typically leads to lower usage rates than including that individual by default and requiring active refusal (i.e., 'opting out').[8] The behavioral findings from this research suggest that creating a standardized, default network of preparedness staff can improve training coordination, preempt disjointed actions, and potentially aid information security. According to FEMA, organizations working in the space should also rigorously test their action protocols, including data collection and evaluation.[9,10] Despite the risks and challenges, technological advances present an opportunity for emergency management, preparedness, and response. What remains to be seen is how government, private hospital networks, technology providers, and other emergency preparedness stakeholders will approach the task at hand: will the evolution be driven by reaction and adjustment, or will there be a proactive approach to cybersecurity, patient data integrity, and first response communication? Let us hope for the latter.

[8] "Do Defaults Save Lives?", Science Magazine.November 2003. http://science.sciencemag.org/content/302/5649/1338

[9] "Nationwide Emergency Alert System Test Planned for September 27", Federal Emergency Management Agency. September 2017. https://www.fema.gov/news-release/2017/09/25/nationwide-emergency-alert-system-test-planned-september-27

[10] "Citizen Corps Personal Behavior Change Model for Disaster Preparedness", U.S. Department of Homeland Security. Fall 2006. https://www.nationalservice.gov/sites/default/files/resource/citizen_prep_review_issue_4.pdf

Research Methodology

GBC and The Cadmus Group LLC launched a qualitative research campaign in July 2017. From August 2017 to September 2017, GBC conducted a series of interviews with federal and state-level leaders in emergency preparedness and response. The list of featured interviewees is as follows:

Jeff Bryant — Director of the Division of Emergency Operations at the Centers for Disease Control and Prevention (CDC)

Dane Matthew — Director of Emergency Preparedness and Response at the Colorado Department of Public Health and Environment

Brendan McCluskey — Director of Emergency Preparedness and Operations at the New Jersey Department of Health

Elizabeth Van Nostrand — Assistant Professor of Health Policy and Management and Director of the JD/MPH Program, University of Pittsburgh

About Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

About Cadmus

Cadmus provides professional consulting services that help clients achieve their goals and create social and economic value today and for future generations. By applying exceptional technical expertise and a highly collaborative approach, we deliver customized solutions to our clients that address complex challenges in energy, homeland security and all-hazard preparedness, climate, the natural and built environments, sustainable transportation, public health, and international development. Cadmus' more than 600 consultants serve government, commercial, and nongovernmental organizations around the world.

Sponsored perspective provided by
Nitin Natarajan — Principal, Homeland Security Sector, Cadmus