EMERGENCY MANAGEMENT
STRATEGY AND LEADERSHIP IN CRITICAL TIMES
FALL 2017

The New Normal?

What Hurricane Harvey and other recent storms tell us about flood control and insurance.

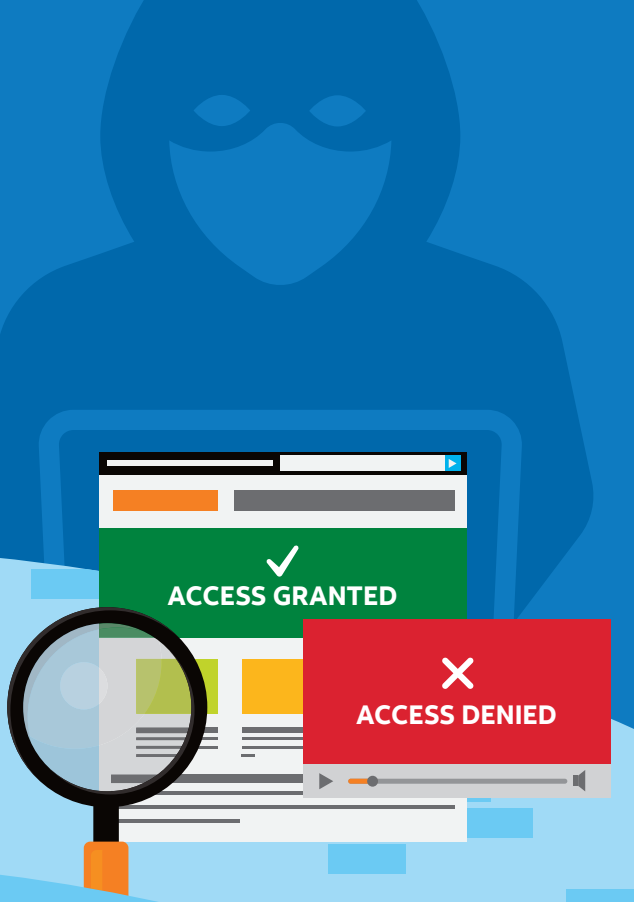
A PUBLICATION OF e.REPUBLIC | ISSUE 4 VOLUME 12 | EMERGENCYMGMT.COM

PROTECTING THE PUBLIC SECTOR FROM RANSOMWARE

State and local government agencies are being held hostage by malicious adversaries and software designed to steal data.

How prepared is your organization to deal with a ransomware attack?

Take 3 minutes to learn more:
att.com/govsecurity



AT&T FIREWALLS

Fully managed security services to help prevent unauthorized access to your network

AT&T THREAT MANAGER

At-a-glance, situational threat awareness for multiple sites and "state of the org" view

AT&T CYBERSECURITY CONSULTING

Lifecycle approach to vulnerability, threat management and path to compliance

AT&T SECURE EMAIL GATEWAY

Best in class e-mail filtering and threat detection

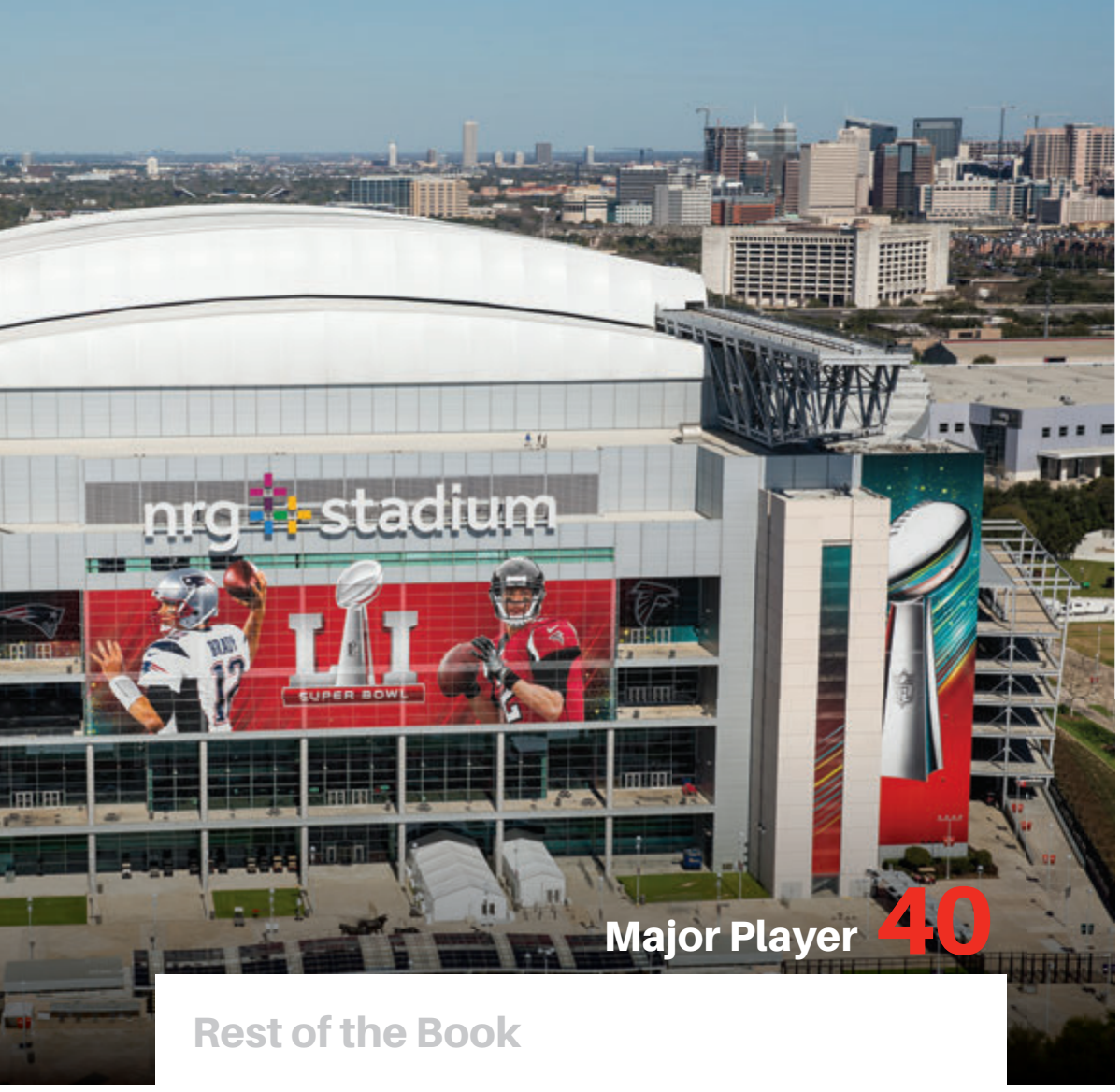
All AT&T Cybersecurity solutions are powered by AT&T Threat Intellect.

AT&T

Contents

Features

SHUTTERSTOCK.COM, COVER IMAGE: SHUTTERSTOCK.COM



WIKIPEDIA

Major Player 40

Rest of the Book

Emergency Management (ISSN 2156-2490) is published quarterly by e.Republic Inc. 100 Blue Ravine Road, Folsom, CA 95630. Periodicals Postage paid at Folsom, CA and additional offices. Postmaster: Send address changes to Emergency Management 100 Blue Ravine Road, Folsom, CA 95630.

100 Blue Ravine Road, Folsom, CA 95630
Phone: (916)932-1300 Fax: (916)932-1470
www.emergencymgmt.com

A publication of e.Republic

Hurricanes, floods, and other disasters. It can't happen here?

Hurricanes Harvey, Maria, and Irma are every emergency planner's wake-up call. We've witnessed the heart-breaking destruction and suffering. **If you wait, it's too late!**

Try for yourself and see why Easy Meal and Mountain House Emergeny Meals are fast becoming the first choice for emergency food planning systems. Plus Easy Meal is your solution to CMS-3178F compliance.

easymeal FOOD SERVICE

easymealfoodservice.com

Best for large group cafeteria-style emergency meals.

MOUNTAIN HOUSE

mountainhouse.com

Best for highly mobile, personal emergency meals.

Call for your FREE sample!

OFD FOODS
800.547.0244

By Carroll G. Robinson and Michael O. Adams

Next Time

It is never too early to start planning for the next time.

Harvey has shown all of us that we need more than the Ike Dike (a coastal barrier proposed after Hurricane Ike in 2008) to protect homeowners and businesses in Houston and Harris County from flooding caused by rainfall.

Imagine how much worse it would have been if Harvey had come ashore far enough north to have hit Houston with higher wind speeds and heavier rainfall?

It's time for elected officials, in our region, to move from planning for flood control to developing a plan to eliminate flooding in Houston and across Harris County and the rest of the region.

> "It's no longer acceptable to be reactive to a storm."

It's time for a regional drainage enhancement and flood elimination district. This effort should be built on Senate Bill 1269 filed by state Sen. Borris Miles during this year's 2017 Regular Session of the Texas Legislature. Gov. Greg Abbott should call the Legislature back for a second Special Session later this year (or early next year) to create the flood elimination district as well as authorize and fund development of a Texas Gulf Coast hurricane resiliency, evacuation and recovery plan.

Some people are going to say it's impossible to eliminate flooding in Houston and Harris County, but that mindset means we have to be willing to lose tens of thousands of homes and businesses to flooding from the rainfall produced by a hurricane or tropical storm.

I don't believe we have to settle for the status quo. Japan and San Antonio have built tunnels to help improve drainage and to better protect against flooding.

If Houston could dig the Ship Channel and help send men to the moon and bring them back, the engineers in our city can design a plan to keep Houston drier than it is now even when Harvey did not directly hit the city.

It is time to issue debt against the city's drainage fee to generate the revenue needed to speed up construction of existing flood control projects and to develop a major flood elimination project. We also need to upgrade the city building code. We must do that now to protect against future high-speed wind damage. We were blessed to not have had serious widespread, high-speed wind issues this time.

Additionally, as the city prepares for the 2020 Census, the Planning Department should develop a database of all Houstonians who would need help in the event of an evacuation in response to a natural or man-made disaster. Harris County and the Houston-Galveston Area Council should also develop similar databases.

Our region also needs a coordinated inventory of water rescue equipment and high-water vehicles as well as trained personnel and joint water rescue preparation exercises.

Our electric grid withstood a lot of punishment but still needs to be made more resilient and redundant. In addition to incentivizing and encouraging "high and dry" backup generators at individual businesses and homes, the city should partner with electric battery technology companies to hardwire backup electric battery capacity into our local grid at strategic locations like Los Angeles is currently doing with Bloom Boxes.

In the last 16 years, we have been hit by Tropical Storm Allison (2001), Hurricane Ike (2008) and now Hurricane/Tropical Storm Harvey. Three times should be enough for us to have learned our lesson. It's now time to use what we have learned to pass our next test whenever it comes. It's no longer acceptable to be reactive to a storm. It's time for us to be fully proactive.

Robinson and Adams are members of the faculty of the Political Science Department at Texas Southern University in Houston.

Questions or Comments?

Please give us your input by contacting our editorial department at editorial@emergencymgmt.com, or visit our website at www.emergencymgmt.com.

FIRST RESPONDERS *first* NEED *an* EDUCATION

EARN YOUR DEGREE ONLINE
with Waldorf University

Let Waldorf prepare you for an exciting career in emergency management with:

// Emergency Management Certificate
// A.A. Emergency Management
// B.A. Emergency Management
// B.A.S. Emergency Management
// M.A. Emergency Management Leadership

WALDORF UNIVERSITY

waldorf.edu // 877.267.2157

In the News

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

Water from Addicks Reservoir flows into Houston neighborhoods as floodwaters from Hurricane/ Tropical Storm Harvey rise on Aug. 29, 2017.

In this satellite image taken on Sept. 7, 2017, the eye of Hurricane Irma, center, is just north of the island of Hispaniola, with Hurricane Katia, left, in the Gulf of Mexico, and Hurricane Jose, right, in the Atlantic Ocean. Irma, a fearsome Category 5 storm, cut a path of devastation across the northern Caribbean, leaving at least 112 dead in Florida and the Caribbean, and thousands homeless after destroying buildings and uprooting trees. Following Irma were hurricanes Jose and Maria.

Social Media Apps Should Be in Disaster Kits

With floodwaters at four feet and rising, a family in Houston abandoned their possessions and scrambled to their roof during Hurricane/Tropical Storm Harvey to sit with their pets and await rescue. Unable to reach first responders through 911 and with no one visible nearby, they used their cellphones to send out a call for help through a social media application called Nextdoor.

Within an hour, a neighbor arrived in an empty canoe large enough to carry the family and their pets to safety. Thanks to a collaboration between The Conversation and Nextdoor, we learned of this and hundreds of similar rescues across Harvey's path.

This story illustrates the power of systems like Nextdoor, an app designed to make communication between neighbors easy. Survivors in Houston have been using social media platforms such as Facebook, Nextdoor and Twitter to connect to rescuers, organize food and medical supplies, and find places for people to stay.

Everyone knows that they should have batteries and three days of water and food on hand as extreme weather events roll through. But in our view, friends and social media platforms reachable by phone are equally important, because they could be lifesavers.

Many people assume that standard emergency services — such as the 911 system, police, firefighters and FEMA — will rescue them from disasters. While these are critical services during normal times, they can become literally and figuratively swamped during major hurricanes and floods, as we saw in Houston during Harvey.

SHUTTERSTOCK.COM

What Tech Is the American Red Cross Using?

The American Red Cross and UPS teamed up to launch a week-long test of a new disaster relief program in September. They used an unmanned aerial vehicle (UAV) to assess the damage in Houston from Hurricane/Tropical Storm Harvey to determine which areas need more immediate assistance. This was to help the Red Cross more efficiently deploy its response teams. The program used a UAV created by Massachusetts-based company CyPhy Works. Connected to a generator, the CyPhy UAV can operate for much longer than the average drone, and can provide extended visibility from 400 feet up in the air thanks to its 30x zoom camera. Success of this pilot program could lead to more use of UAVs in future disaster response initiatives, including response to the impact of Hurricane Irma, which made landfall in Florida in early September.

SOURCE: THE CONVERSATION

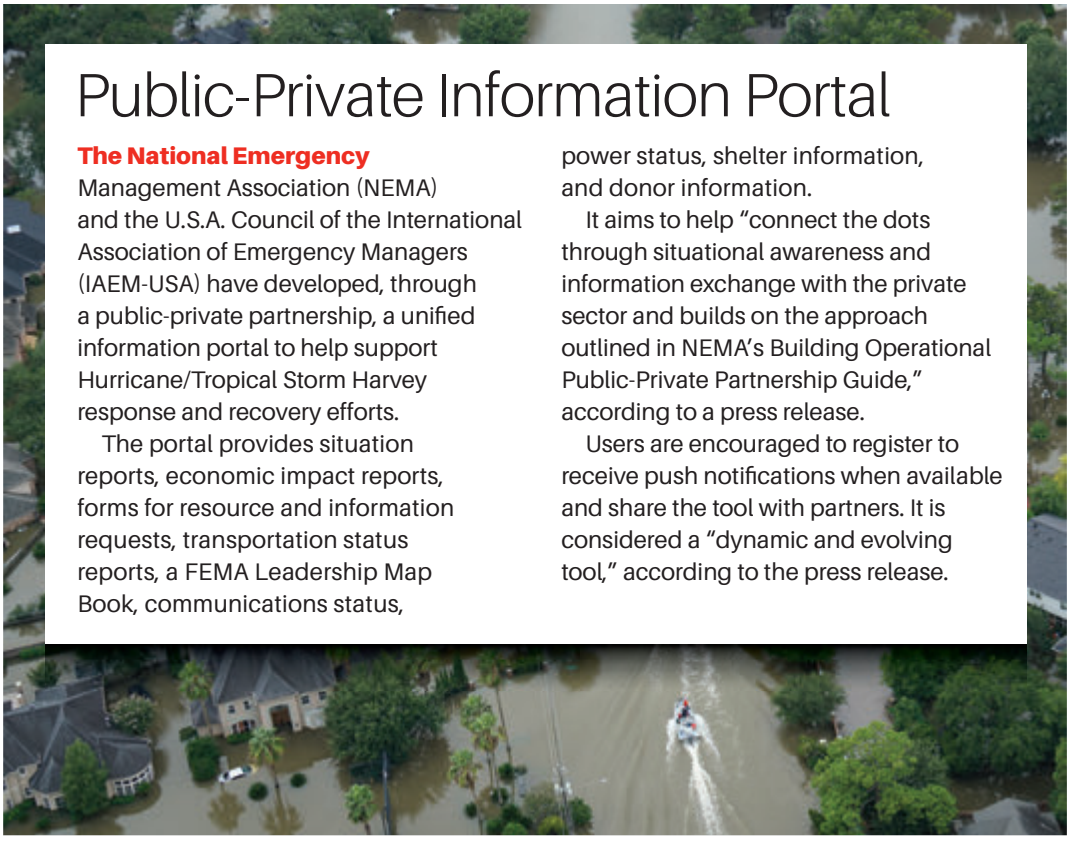
Public-Private Information Portal

The National Emergency Management Association (NEMA) and the U.S.A. Council of the International Association of Emergency Managers (IAEM-USA) have developed, through a public-private partnership, a unified information portal to help support Hurricane/Tropical Storm Harvey response and recovery efforts.

The portal provides situation reports, economic impact reports, forms for resource and information requests, transportation status reports, a FEMA Leadership Map Book, communications status, power status, shelter information, and donor information.

It aims to help "connect the dots through situational awareness and information exchange with the private sector and builds on the approach outlined in NEMA's Building Operational Public-Private Partnership Guide," according to a press release.

Users are encouraged to register to receive push notifications when available and share the tool with partners. It is considered a "dynamic and evolving tool," according to the press release.



SHUTTERSTOCK.COM

DISASTERS DON'T
PLAN AHEAD.

YOU CAN.

DON'T WAIT. COMMUNICATE.

Talk to your loved ones about how you are going to be ready in an emergency.

VISIT READY.GOV/PLAN.

Ad Council Ready® FEMA

TERROR ON

SHUTTERSTOCK.COM

THE FARM

NO MATTER WHAT THEIR CAUSE, MAJOR AGRICULTURAL DISEASE OUTBREAKS PUT THE NATION AT RISK.

BY MADELINE BODIN

THE POULTRY FARMERS OF IOWA COULD SEE IT COMING, ALMOST LIKE A STORM ON THE HORIZON. AVIAN INFLUENZA STRUCK MINNESOTA – THE NATION'S LARGEST TURKEY PRODUCER – FIRST, STRIKING HARDEST WHERE TURKEY PRODUCTION WAS THE DOMINANT INDUSTRY. IT THEN JUMPED TO MISSOURI, THEN ARKANSAS, THEN NORTH TO KANSAS AND NORTH AGAIN TO SOUTH DAKOTA, DEFYING THE MIGRATION PATTERNS OF THE WILD BIRDS SUSPECTED OF CARRYING THE VIRUS, BEFORE STRIKING MINNESOTA A SECOND TIME. IT SICKENED AND KILLED BOTH TURKEYS AND CHICKENS.

Iowa is the nation's leading egg producer, with 60 million birds laying 15 billion eggs per year, or one out of every five produced in the United States. The state ranks ninth in the nation in turkey production.

In Iowa, avian influenza struck a turkey farm first, then a huge egg farm with more than 4 million layers. Before the outbreak subsided, 77 properties in Iowa were hit. Millions of birds were killed, either by the virus or in the attempt to keep it from spreading. Across the country, it had affected nearly 50 million birds in 21 states.

Is this what agricultural terrorism would look like in the United States? It might.

"The United States is underprepared for biological threats," said the 2015 report from the Blue Ribbon Study Panel on Biodefense. "Nation states and unaffiliated terrorists (via biological terrorism) and nature itself (via emerging and re-emerging infectious diseases) threaten us," it continued. "While biological events may be inevitable, their level of impact on our country is not."

Although the United States has not experienced an act of agroterrorism by foreign terrorists, this avian influenza event is not made up. It's what happened when an avian influenza that is particularly harmful to birds, known as a highly pathogenic avian influenza (HPAI), struck the heartland in spring 2015. There are several different strains of HPAI, including the H7N9 strain that, according to the World Health Organization (WHO), has killed dozens of people and sickened hundreds in China since 2013.

The 2015 outbreak was not an act of terrorism, but an animal disease outbreak with natural causes. It was the worst animal disease event in U.S. history, according to the U.S. Department of Agriculture (USDA) Animal and Plant Health Inspection Service (APHIS) Veterinary Services. However, small outbreaks of animal diseases — killing a few dozen or a few hundred animals — are common.

During the 2015 Iowa avian influenza outbreak, "every day you would wake up and say, it can't get worse than this," says Robin Pruisner, agriculture security coordinator for the Iowa Department of Agriculture and Land Stewardship and the state's incident commander for the outbreak. "And day after day, week after week, it got worse."

Diseases of plants and animals are a threat to national security, whether or not the outbreaks are caused by terrorists. Food safety policies that defend against accidental and natural disease outbreaks should also limit the harm done by a biological terrorist attack against agriculture.

A heightened awareness of the threat of bioterrorism and agroterrorism has been part of America's general increased alertness about terrorism after the 9/11 attacks, and the anthrax attack that followed a few weeks later. In that anthrax attack, five people died and 17 were sickened when weaponized anthrax was sent in envelopes through the U.S. Postal Service.

"EVERY DAY YOU WOULD WAKE UP AND SAY, IT CAN'T GET WORSE THAN THIS, AND DAY AFTER DAY, WEEK AFTER WEEK, IT GOT WORSE."

Robin Pruisner, agriculture security coordinator, Iowa Department of Agriculture and Land Stewardship

In June 2017, President Trump signed the Securing our Agriculture and Food Act, which puts the Department of Homeland Security's assistant secretary for health affairs in charge of coordinating efforts to prevent and respond to agroterrorism attacks. It's one of several laws enacted since September 2001 to address bioterrorism in general and a handful of laws to address agroterrorism specifically.

In response to the signing of the act in June, Rep. David Young, R-Iowa, who introduced the bill to Congress, said, "Agroterrorism is a real threat, and this legislation takes the necessary and critical steps to protect America from high-risk events which pose serious threats to our food, across Iowa and the United States."

THE RISKS

Though there is general acknowledgment that a biological agroterror attack could harm the nation's economy and food supply, as well as possibly cause human illness, the likelihood of an attack is not clear.

In 2002, "U.S. Navy SEALs found a list of pathogens and a schematic in an Afghanistan cave that al-Qaida planned to use to produce bioweapons. In addition to six human pathogens, 10 pathogens targeted food, six targeted livestock and poultry, and four targeted crops," wrote former U.S. Sen. Tom Daschle and chairman of the Joint Chiefs of Staff Richard B. Myers in a 2016 *U.S. News & World Report* article.

This story has been repeated many times, in articles and by experts in agroterrorism, although a source for the information is not given. The validity of this vivid and chilling terrorist threat to American agriculture rests on the credibility of Daschle and Myers.

Another consideration is how easy it would be to attack that nation's agriculture system with a disease organism.

"We tend to think of bioweapons in the human world, in warfare," said William Karesh, executive vice president for health

and policy for the nonprofit EcoHealth Alliance and adviser to the Blue Ribbon Study Panel on Biodefense. "It's a sophisticated process to take a naturally occurring organism and make it weaponizable. But some of these animal diseases are caused by viruses that can survive for months or years without having to do anything special to them."

The consequences of an agroterror attack would be grave, Karesh said. It could be devastating to the economy, because agriculture makes up 5.5 percent of the country's gross domestic product and employs 11 percent of Americans. It could cause food shortages and even starvation.

It could also harm human health. Bioweapons have been created from diseases shared by animals and human beings, such as anthrax, brucellosis, histoplasmosis, plague, Q fever, rabies and tularemia. The direct threat to human health and the association with bioweapons increases the fear associated with agroterrorism.

On the other hand, naturally occurring or accidentally caused animal disease outbreaks are so common that they are drained of some of their terror. Only the largest outbreaks make the national news. Some agroterrorism experts have said that this makes an attack less valuable to terrorists.

ANIMAL DISEASE RESPONSE

The threat of even natural or accidental disease outbreaks is so serious that many diseases of animals and plants are mandatory to report at local, state, federal and international levels. The World Organisation for Animal Health (OIE), an intergovernmental organization with 180 member countries, collects animal disease data from around the globe.

Veterinarians who work with farm animals in the U.S. are trained, and reminded, to contact the USDA assistant district director (ADD) for their state or their state veterinarian's office when they encounter any one of a long list of diseases, including anthrax, foot-and-mouth disease, and rabies, as well as lesser-known diseases like vesicular stomatitis.

USDA ADDs and state veterinarians are the people with top-of-mind knowledge of animal diseases, from how contagious they are among animals to how dangerous they

SHUTTERSTOCK.COM

are to humans to how to contain them. For emergency managers, they are people well worth getting to know before an outbreak.

"Foot-and-mouth disease is one of my biggest concerns," said Ron Snyder, a consultant based in Brooklyn, Iowa, and a trainer who developed the DHS-certified curriculum for the AgTerror Emergency Responder Training program. Foot-and-mouth disease is highly contagious. Symptoms in cattle, hogs or sheep don't show up until five to seven days after exposure, Snyder said, which is more than enough time for animals or equipment to be transported from coast to coast.

A 2001 outbreak of foot-and-mouth in the United Kingdom showed just how devastating this disease could be. Millions of animals were slaughtered to stop a disease that does not affect people and doesn't kill adult animals, but destroys their economic value. The effort cost the equivalent of $10 billion, according to the BBC. The outbreak not only hurt farmers and stopped UK meat exports, but also caused a drop in tourism.

What makes responding to an animal disease outbreak so tricky, Snyder says, is that it brings together so many groups that don't normally work together, including law enforcement, public health officials, medical personnel, veterinarians, agriculture officials, farmers and producers, and hazardous materials teams. "We can't silo information," he said.

EMERGENCY MANAGEMENT ROLE

Pruisner, the Iowa agriculture security coordinator, said she works closely with the state's county emergency managers and the state Homeland Security and Emergency Management Department. The big difference between responding to a natural or unintended disease outbreak and a criminal or agroterrorism attack is that in the latter, you need to preserve evidence for law enforcement. In both cases you will likely be involved in setting up quarantines and helping dispose of many animal carcasses.

"Emergency managers tell me that all emergencies are local, and if they need help, they will reach out," she said.

But a disease outbreak is a regulatory matter, she added. If the disease is on the federal reporting list, and conditions warrant it, the response is going to come from the federal government. "I think this was hard for the locals to buy into because it is the opposite of how they handle things."

Iowa had plans for dealing with a major animal disease outbreak, Pruisner said. It wasn't enough. "The best-laid plans go awry. You can plan and exercise and you will still find yourself in uncharted territory."

In Iowa, one place the plans went off course was in disposing of millions of poultry carcasses. The plan called for farmers to use one of several means of sanitary disposal: landfill, burial on site, composting or incineration.

But some landfills refused the carcasses, Pruisner said, either because they were already full or were concerned about spreading the disease to nearby farms. Not all farmers could bury the carcasses because, with a shallow water table, it risked contaminating local drinking water supplies. Few farmers chose incineration. (News reports say that there simply weren't incinerators in the area.) So many farmers were composting and the area ran out of the wood chips, cornstalks and other carbon sources that were needed to mix with the carcasses.

Through the spring of that year, USDA teams were coming into the state for 28-day deployments. In animal health emergencies, the USDA depends on volunteer veterinarians who are trained ahead of time and become temporary federal employees when they are called into service.

"We had the red team, the indigo," Pruisner said. "Each team had trained together and had their own way of doing things." Some farmers dealt with several teams during the crisis, each with different procedures and a different bedside manner. "We needed a better transition and more consistency in the field."

THE CRISIS AND LEGISLATION

Farmers complained. The egg and turkey producer associations complained. They said that state and federal authorities did not take action soon enough, that the instructions to farmers were confusing, and that the cleanup took too long. In news reports, the USDA said it would change things, particularly providing more consistent points of contact between farmers and the agency.

Pruisner said that in the future, the state will provide a liaison so that individual farmers can reach the same person throughout an emergency. It also put together a book describing procedures in the first few hours and days after avian influenza is detected on a farm.

But for Rep. Young, enough was enough. In his press release announcing the president's signing the bill he introduced into law, he hints that the shortcomings of the avian influenza response inspired him to introduce the legislation that would become the Securing Our Agriculture and Food Act, which mandates that the Department of Homeland Security (DHS) coordinate responses to agroterrorism.

The release said: "First introduced in 2016, and then again in January of this year, Congressman Young's legislation addresses concerns brought to light after Iowa suffered the largest animal disease outbreak in state history, when the 2015 avian influenza outbreak wiped out millions of layer hens, turkeys and backyard flocks. Response efforts revealed problematic preparedness concerns and breaks in the federal government's ability to communicate with stakeholders and react quickly to large-scale animal disease outbreaks. This disaster also raised concerns among farmers, producers and ag experts about whether our nation would be able to capably share information and respond to agroerrorism threats and attacks, ultimately an attack against our nation's citizens."

That may sound like Young set out to punish the USDA for its failure in the 2015 avian influenza outbreak by handing over the reins to DHS in the event of an agroterror attack, but, through a spokesman, Young said that isn't so. Previous laws put the DHS assistant secretary for health affairs in charge of the response to other forms of bioterrorism. This law makes sure that agroterrorism is included. Sen. Pat Roberts, R.-Kan., one of the bill's Senate sponsors, agrees that this was the goal.

Young said that DHS and the USDA must work together for the nation's response to be effective.

Because it brings together so many government agencies and so many different types of expertise, responding to agroterrorism takes an exceptional level of coordination and communication. In the end, it means meeting the challenges of human nature as much as it means defeating a disease.

"At times," Pruisner said. "I don't have words for 2015."

madelinebodin@gmail.com

Hacking Health Ca

re

SHUTTERSTOCK.COM

Protecting the nation's health-care system against cyberattacks. By Margaret Steen

The scenarios are chilling: A busy hospital suddenly cannot use any of its electronic medical records or other computerized systems. The victim of a ransomware attack, the hospital will not regain access without paying those who locked down the records — if at all.

At another hospital, hackers find a way to connect to the software that controls IV pumps, changing their settings so they no longer deliver the correct doses of medication.

Cybersecurity experts say these are among the situations they worry about when they consider the health-care industry — which, with its reliance on technology and a wealth of data, is increasingly a target of cybercrimes.

"We have seen in recent years an escalation in the risk to health-care organizations from cyberthreats," said Steve Curren, director of the Division of Resilience in the Office of Emergency Management, part of the U.S. Health and Human Services Department's Office of the Assistant Secretary for Preparedness and Response. "Since 2014, we have had 10 distinct breach incidents of health-care organizations where the breach resulted in the compromising of more than 1 million patient records."

And starting around 2016, attackers ramped up ransomware attacks against health-care systems. "That has been very disruptive," Curren said, sometimes forcing hospitals to implement emergency procedures.

Ransomware attacks have "impacted health care directly," said Monzy Merza, head of security research for Splunk, an enterprise software company. "There were several reports of UK hospitals unable to administer X-rays. The computer equipment attached to the X-ray machines was compromised and attacked by ransomware and rendered inoperable for some period of time."

Experts say there are a number of reasons for the increased risk — and challenges, some unique to health care, in mitigating it.

"Cybersecurity is somewhat of a nascent discipline," Merza said. "We're still learning. Manufacturers are learning how to operate in this new world. The same is true for the operators and owners of these technologies, who are also learning what the best practices are and how to manage them."

There are several reasons the health-care industry makes an attractive target for cybercrimes:

Lots of data. People launch cyberattacks for a variety of reasons, said Phyllis A. Schneck, managing director and global leader of cybersolutions for Promontory Financial Group, an IBM Company, and former chairman of the National Board of Directors of the FBI's InfraGard program. Some are simply having fun; others are deliberately trying to destroy infrastructure. But a common reason is to steal intellectual property or personal information for financial gain. The health-care sector is "a resource-rich environment" for those looking for information due to the wealth of information health-care providers store: family history, medical history, financial information.

"There's a street value to people's personal information, and the health-care sector is an excellent source of it," Schneck said. Trade secrets can also be sold for profit.

Health-care organizations also have a lot of information that can be valuable to those who want to commit health insurance fraud, Medicare fraud or identity theft, Curren said.

Ransomware attacks are yet another way to make money.

"A lot of the bang for your buck is in locking up the system: Send in malware that freezes all the computers in the hospitals, then say, 'I'll send the code to unlock this if you send money,'" said Deborah A. Levy, a retired captain with the U.S. Public Health Service and currently professor and chair of the epidemiology department at the University of Nebraska Medical Center's College of Public Health. With the move toward electronic health records, the industry has become a bigger target.

Individual medical records may also be attractive if they include sensitive information about celebrities, for example, though in general there is less of a market for them.

Connections among diverse organizations. "The reason we're seeing more of this now is because of the connectivity of networks and devices to the network," Merza said. "There are clear advantages to connected devices — automation, information sharing, knowledge enrichment, contextualization. But with that network connectivity, you're opening yourself up to attack."

Organizations within the health-care sector also need to communicate with each other, so even if a large insurance company or hospital is able to secure its data, it may still be vulnerable when it shares connections with smaller organizations that have fewer resources for cybersecurity.

"We have a very diverse sector," Curren said, ranging from large health insurance organizations with a lot of resources to very small clinical practices.

An open culture. "Health care has an open, sharing culture — as is appropriate to support its primary mission — but this culture also complicates the issues of security and privacy," said the June 2017 *Report on Improving Cybersecurity in the Health Care Industry*, produced by the Health Care Industry Cybersecurity Task Force of the U.S. Department of Health and Human Services.

This means it has been harder for health-care organizations to secure their data than some other industries.

"They do not have really good security technologies and privacy policies in place," said Niam Yaraghi, a nonresident fellow with the Brookings Institution's Center for Technology Innovation and assistant professor of operations and information management at the University of Connecticut's School of Business. "They are like the only house in the very affluent neighborhood that doesn't have a security system."

SHUTTERSTOCK.COM

"The first and foremost mission of every health-care organization is to cure the sick and help the patient," Yaraghi said. "If you're being rushed to the emergency department, the first thing in your mind is, 'I hope the physicians at this hospital are really good doctors.' Whether they're going to keep your blood pressure and drug allergies confidential — that's not the first thing you care about. They are in the business of providing medical care to patients; they are not in the business of technology."

Focus on Solutions

The results of a breach for everyone involved in the health-care industry — hospitals, clinics, researchers and patients — can range from annoying to catastrophic.

Patients could be harmed or even die. Many people — both patients and health-care workers — could be inconvenienced by systems going down. And bad publicity could harm clinics and hospitals in areas where consumers have choices.

"It's a competitive business — if a facility has gotten hit, that might influence where the public chooses to go," Levy said.

Prevention is the best solution — but it, too, poses challenges. Experts offer these ideas for shoring up security to prevent or mitigate attacks:

Education and awareness. "In the past, it was much more challenging implementing cybersecurity features because people didn't consider it a must," said Idan Edry, CEO of Trustifi LLC. "They said, 'I've never been hacked, nobody stole any of my information, so I'm fine.'"

Today, those on the front lines of using the more secure systems — including patients and medical professionals — are more aware of the importance of cybersecurity. Continued education will help

ensure that the people who need to use the secure systems are on board.

Simplicity. The more complex a system is, the harder it can be to keep updated to guard against cyberattacks.

"Keep it simple: Don't have too many disparate things where if you make one update it breaks everything else," Schneck said. "The more hot, new devices that you have, the more openings you have."

Backup systems. When cybersecurity systems fail to prevent an attack, good backups can make it easier to recover.

"In the case of ransomware, it's important to have very good backups, so that when something is compromised, you're able to get back up and running," Merza said.

Emergency planning. Cybersecurity may be an emerging challenge, but emergency managers can tackle it by using strategies similar to those they use for other situations. "If a hospital gets disrupted by a cyberincident, it's the same as if it was disrupted by a water main break or a tornado or anything else," Curren said.

Constant vigilance. Both manufacturers and owners of devices bear some responsibility for preventing attacks. Users and operators should be prepared to follow best practices for installing and testing the updates.

"Start with the fundamentals," Merza said. Manufacturers should be constantly evaluating bugs and vulnerabilities of their equipment and sharing that information with owners. "How quickly can manufacturers identify the problem, come up with the fix and distribute the fix to the users of those devices?"

Realistic regulations. Cybersecurity plans need to keep in mind the mission and culture of the health-care industry.

For example, it's easy to say all operators should immediately install all patches. But "sometimes it is not feasible for any number of reasons," Merza said. Government agencies that regulate the systems may be slow with their approval. "The regulatory space is not equipped today to handle the evolving nature of threats and the speed with which technological development is happening. There is an opportunity now for regulatory bodies to work with operators and manufacturers to understand the on-the-field requirements so people can implement them in a reasonable fashion."

Healthy attitude toward risk. It's easy to blame doctors for being reluctant to learn a new electronic medical record system, for example, or update their computers.

"Doctors are geniuses in how they figure out how to help people, but notorious for not being meticulous about cybersecurity," Schneck said.

But it is important for those in charge of cybersecurity to keep the true goals of everyone who uses the systems in mind. Researchers need to be able to share information and produce new drugs. Health-care providers need to be able to exchange patient information. Some security measures may make it hard for health-care professionals to do their jobs. The key is to consider cybersecurity through the lens of risk management, Schneck said.

"It's not the doctor's fault that he is too busy and he thinks that he doesn't have time for remembering a complicated password that cannot be hacked into, not the nurse's fault that she is under so much pressure that she cannot read every email very carefully and figure out that it's a phishing email," Yaraghi said. "I do not blame physicians and people in the health-care industry at all."

Cooperation. So many of the players in the health-care system are connected to each other — hospitals communicate with doctors' offices, pharmacies and insurance companies, for example — that an attack on one entity with weaker security could threaten others.

"There's a real strong sense developing in health care that we have to do this together, and we have to be committed to sharing information with one another to make this work," Curren said. For example, hospitals need to notify each other of attempted attacks so other hospitals can prevent them.

In addition, a long-term solution would be for device manufacturers to "develop products and services that are hard to compromise," Merza said. "The government, the manufacturers and the operators of these devices all really have to work together in the best interests of the public health-care population."

msteen@margaretsteen.com

Government Resources

The U.S. Department of Health and Human Services' Health Care Industry Cybersecurity Task Force came out with a report in June that listed six imperatives for the industry, including developing the technical workforce necessary to help health-care organizations beef up their cybersecurity, and improving information sharing.

"The health-care system cannot deliver effective and safe care without deeper digital connectivity," the report said. "If the health-care system is connected, but insecure, this connectivity could betray patient safety, subjecting them to unnecessary risk and forcing them to pay unaffordable personal costs. Our nation must find a way to prevent our patients from being forced to choose between connectivity and security."

Additionally, the Centers for Disease Control and Prevention has published a Healthcare Organization and Hospital Discussion Guide for Cybersecurity.

COLLABORATING FOR BETTER PUBLIC SAFETY RESPONSE

Real-time mobile communication helps law enforcement agencies respond to community needs more effectively. Have you thought about securing all the endpoints that enable this?

Why Collaboration is Complicated

What should be simple — the ability of law enforcement personnel to exchange information and work together, especially in the field — is often complicated. Effective collaboration among agencies is essential to meet the challenges of public safety, but many communications and workflow systems are more of a hindrance than a help.

Law enforcement agencies need interoperable technologies that will help them address collaboration challenges in the vital areas of communications, responsiveness and operations. Equally important is the IT department's ability to protect agencies from external threats and internal bad actors.

Better communications. Although a land mobile radio system provides value as a collaboration tool, it is often limited by congestion and siloed frequencies. Commanders, team leaders and operations center staff also need the rich information that photos, videos and documents can deliver and to share them securely when needed.

Improved responsiveness. First responders need immediate interoperability and secure mobile capabilities for greater effectiveness. When responding to an emergency, agencies must scramble to contact and dispatch off-duty officers, mobilize support and command staff within the department, and request help from other agencies.

Operational efficiencies and cost savings. Agencies need technologies that enable more efficient collaboration through document workflows that save staff time for processing reports and statements.

How can law enforcement agencies meet these needs with limited budgets? And how can today's mobile technologies be deployed for the greatest operational, collaborative and budgetary impact?

Utilizing Technology to Improve Collaboration

In the past, public safety collaboration was limited to land mobile radios and complex enterprise-level software and hardware systems that ran on desktops and laptops. Documents were traditionally shared over insecure email or public file sharing platforms. Today's collaboration solutions start with standard, consumer-grade mobile devices (iOS or Android) and leverage powerful communication and computing capabilities, and a wide choice of applications.

Mobile devices, along with Windows 10 and Mac OS laptops, offer a modern platform that — when equipped with the right set of tools — empowers officers to access and exchange critical information. The new breed of mobile software solutions support information access and file sharing from any commercial device, automated alerting, presence accounting in emergencies, location mapping, image and video recording, instant messaging and more — along with strong data and application security.

Perhaps the best way to understand the impact of these capabilities is to see how they support communication, decision-making and execution in the day-to-day work of law enforcement.

"For a law enforcement agency, accessing data on the go is critical to a timely response to any crisis. BlackBerry and Mobile Innovations together delivered innovative solutions to the public safety and enforcement market in Canada, the United States and the United Kingdom, enabling productivity of the mobile workforce. With BlackBerry UEM, agencies can manage today's endpoints, apps, content and data with utmost security, prepare for future challenges and start building a safer world for our citizens."

— GARY BAUER, PRESIDENT, MOBILE INNOVATIONS

Reaching Across the Continuum of Public Safety Activities

Mobile technology enhances collaboration at every step of law enforcement work, from the initial response through the close of an incident or case.

Supervisor Awareness
Detailed information, including photos and video, shared instantly from an on-scene officer helps supervisors make precise decisions for incident command. Law enforcement personnel can use the same platform to coordinate activity internally and externally with other agencies, and reach out to stakeholders such as schools, community agencies and the media. All these situational awareness activities are easier when officers in the field use a secure mobile device.

Incident Coordination
At times a situation calls for specialized resources such as a SWAT team and officers who are not on duty or who aren't reachable over the radio system. Mobile alerting allows on-duty and off-duty officers to instantly check-in if available, reducing overall response time. Personnel tracking and presence accounting also help commanders better manage activity across teams and agencies.

Evidence Gathering and Criminal Investigation
When at a crime scene, officers need a secure and robust way to communicate and share documents and images with investigators or collaborate with other public safety personnel. Ordinary text messaging capabilities, email and public file sharing systems are not adequate for this purpose. A mobile messaging platform designed for public safety supports encrypted sharing of text, photos, audio and video with strong controls over access and user management.

Data and Records Management
Secure mobile tools can integrate with existing in-house case management and archiving systems. This allows officers to access data, file forms and reports, and share documents in the field instead of going into an office. An agency benefits from greater data accuracy and rapid information availability, improving investigation and cross-agency efficiencies. Modernized records management reduces cost by eliminating the need to manually enter data and by streamlining work through automated processes for document reviews, distribution and forwarding.

Simplifying Emergency Alerts in Contra Costa County

Located in an earthquake zone and with four oil refineries and two chemical refineries in its jurisdiction, Contra Costa County, Calif., has high concerns for alerting the community about emergencies. "We can now go to one website and, depending on the nature of the hazard, we can activate as few or as many alert tools as we want, all in one place without having to go to multiple platforms or multiple interfaces," says Heather Tiernan, community warning system manager for the county. Sending those alerts is now simpler for county emergency personnel because they use BlackBerry AtHoc's integrated online system.

Prosecutor's Office
Control over content sharing is a key concern in maintaining evidence integrity for prosecution. Digital rights management (DRM) controls provide complete file access logs and activity by user device and IP address, showing who accessed the file, what they did and when they did it. In contrast, consumer tools for file sharing and collaboration aren't enterprise grade and don't meet the certifications or requirements for high-security technology implementations.

Making Collaboration Easy and Secure

Law enforcement is under tremendous pressure to minimize crime, pre-empt terrorist attacks and respond to incidents faster. Meeting these needs requires a robust set of mobile tools that supports secure access, communications and features across the spectrum of response, investigation and prosecution.

A high-security mobile solution helps police forces simplify interoperability, streamline operations and reduce costs. Yet perhaps the biggest impact comes from an agency that is better able to deliver quick and effective response to the community.

BlackBerry envisions to secure all mobile communications to build a safe and secure world.
For more information, please visit https://us.blackberry.com/enterprise/industries/public-safety

BlackBerry®

This piece was developed and written by the Emergency Management Content Studio, with information and input from BlackBerry.

Will it cover rural areas? Will it be just for data? Will it really be dedicated to emergency responders?

By Adam Stone

Since Congress breathed life into FirstNet in 2012, emergency managers have been subject to a deluge of information about developments on the nation's broadband first responder network. Bolstered by a $7 billion allocation from Congress, the First Responder Network Authority has contracted with AT&T to build the network and as of this writing, 23 states and territories had signed on to participate.

Despite all that has been said and written, and even with the project well underway, many in the emergency community remain unclear about some of the basic facts surrounding FirstNet. Will it cover rural areas? Will it be just for data? Will it really be dedicated to emergency responders?

We went to FirstNet executives for clarification, and polled a panel of experts for their views. The result: five things you need to know about FirstNet today.

SHUTTERSTOCK.COM

CLARIFYING
STNET

Will FirstNet be a data-only network? What else will be available?

FirstNet will have voice capabilities from the start, but not all the voice you want. That will take a little while.

"The network will offer 4G LTE voice and data capabilities over a high-speed network," said FirstNet President TJ Kennedy. "Voice over LTE has become very robust. A few years back, people weren't sure if LTE would be there, but it really is. So FirstNet will kick off with voice and data."

Technical progress in the past few years has made voice over LTE sufficiently robust to support first responder needs, he said. But fully fledged voice for first responders — defined as "mission-critical" voice — won't arrive on FirstNet until about 2019.

The 3rd Generation Partnership Project standards body approved a definition for mission-critical push-to-talk functionality in mid-2016. It supports a "discovery" feature that will allow users to know when they are in range of one another, and a relay capability to keep out-of-coverage users connected.

Even without these robust capabilities, FirstNet will have basic voice services. "You will have the ability to do phone calls, you will have the ability to do push-to-talk over cellular. Just like you use Skype and FaceTime, you will be able use that to make phone calls," Kennedy said.

When mission-critical voice becomes available, users will still have the option of sticking with their existing land mobile radios. "It will be a service offered in the FirstNet network," said FirstNet Chief Technology Officer Jeff Bratcher. "It will be up to public safety whether to use that feature or not. If they are happy with their land mobile radio systems, we are not mandating that they switch to mission-critical push-to-talk."

Experts predict that many first responders may choose to stick to existing voice systems, whether to get the most out of past investments or out of concerns over adopting a new technology. Given the typical delays involved in bringing any new standard to fruition, "it's critical that we not divest from land mobile radio communications until such time as we get true mission-critical voice communication," said Robert LeGrande, founder of The Digital Decision consulting firm.

Others note that, as much as first responders may be eager to see mission-critical voice built into FirstNet, the network's foremost purpose still is to make data the operational core of future first response.

"When you consider video and high-resolution images, that takes a considerable amount of bandwidth, so that data capability is going to have considerable value to incident management," said Yucel Ors, National League of Cities federal advocacy program director for public safety.

Will there be rural coverage?

Yes. Eventually.

A former Utah state trooper, Kennedy has worked a landscape where broad swaths lacked communications coverage of any sort. Sensitive to rural needs, FirstNet asked potential builders to propose a milestone formula, with rural coverage to be built out roughly 20 percent at a time over the first five years. "AT&T has a solution that does exactly that," Kennedy said.

The five-year plan will use AT&T's existing $180 billion in telecom infrastructure as the fastest way to get FirstNet into the countryside. "If we were to build a new network from scratch, that would take more than five years. It takes building permits and site location acquisition. It's costly and time-consuming and it doesn't happen overnight," Kennedy said.

The exact rollout of FirstNet beyond the cities and suburbs will depend on states' preferences. "We've worked with states as part of the RFP process to have them indicate their priorities based on where they actually have public safety calls. It's more than just population, it's where they have emergency

DAVID KIDD

responses," Kennedy said. "So AT&T leveraged that data to cover as much as possible while keeping the costs low. It's all about getting the most cost-effective solution while still going as far into rural as we can."

FirstNet conducted outreach over four years to determine specific rural needs. "We talked to public safety agencies, asking them where the key areas are that they know they need coverage," Bratcher said. "We drove all that collective input into our RFP so that any potential bidder understood where the key areas would be, where a state needs coverage."

Emergency experts have endorsed this approach. "If an EMS agency identifies an area where they receive frequent calls — a nursing home in a rural area — AT&T will work to move the deployment of coverage in that area up on their schedule," said Ray Lehr, a former Maryland single point of contact/statewide interoperability coordinator and retired assistant chief of the Baltimore City Fire Department.

LeGrande said this approach, to target deployment by need, represents a realistic solution to a complex problem. "In some rural areas, we shouldn't put coverage: At the top of mountains where you literally have no one there, not even a ski resort, it's just not feasible," he said. He encourages the use of "deployables," mobile communications pods that can extend the reach of a network on an ad hoc basis. "You need a solid deployable strategy such that you can get to the most rural areas in a reasonable amount of time. No network can get to every inch of every portion of every part of our country. You have to take the network with you."

That's just what FirstNet has in mind. Kennedy said the AT&T contract includes a "robust plan" for the use of deployable assets to ensure rural connectivity. Bratcher said that AT&T has developed 72 deployable units — cells on wheels and satellite-capable nodes — that will be dedicated to FirstNet. Users will also have access to AT&T's existing inventory of more than 400 deployable systems.

Is FirstNet in fact a "dedicated public safety network" and what does that mean?

Well, that was the promise all along. So why the confusion? It's because AT&T is leveraging existing assets, essentially piggy-backing FirstNet on top of its

APIMAGES.COM

Verizon Provides Another Option

FirstNet has given AT&T the contract to build and operate the nation's first dedicated broadband public safety communications network. But Verizon wants emergency managers and first responders to know that they still have other options.

A longtime player in the public safety communications arena, Verizon doesn't intend to surrender its position quietly. Instead, the carrier plans to build its own dedicated broadband core for emergency communications, which it will offer as an alternative to FirstNet. Executives say this will give end users greater flexibility and ultimately enhance the FirstNet mission.

"Our commitment to public safety is as strong as ever," said Mike Maiorana, senior vice president of public sector for Verizon Enterprise Solutions. "Verizon fully intends to complement and enhance the FirstNet value proposition. We plan to be very relevant."

In addition to its ongoing multibillion-dollar network investments, Verizon plans to build and operate "a private network core dedicated to public safety communications that will operate separate from our commercial core," Maiorana said.

The carrier already is giving emergency service providers priority access to its commercial network, as it did during the recent Texas and Florida hurricanes. By the end of the year, it plans to offer pre-emption, the ability of first responders to claim use of the telecom network in times of crisis. "We want to make sure they have the connectivity they need when they need it most," Maiorana said.

In building the public safety core, Verizon says it is looking to enhance rather than to undermine FirstNet's efforts. The carrier says that by making its core interoperable with FirstNet, it will bolster the mission of public safety communications by giving emergency agencies more options.

"We see a meaningful opportunity to work with FirstNet, to accelerate their mission," Maiorana said. "One size does not fit all. Customers want choice and they want options."

Why might a state pursue the Verizon broadband option over the FirstNet-sanctioned AT&T offering? A number of variables come into play. "They may prefer one provider over another based on their past experience, based on coverage, based on contract options," Maiorana said.

He noted that states need not opt out of FirstNet in order to sign on to Verizon's offering, nor will they be required to invest in construction of the network.

commercial architecture. That has some folks worried. Will the network truly belong to first responders above all others?

"If public safety needs the network, they need to be able to pre-empt anybody else on the network," Ors said. "So if there are secondary users they will have to be subject to pre-emption. FirstNet will have to figure out how to do that. That was the whole point of FirstNet. Commercial providers were not willing to provide that in the past, so we need to see FirstNet do this. First responders get first use of that network."

Absolutely, Kennedy agreed. "It is going off the same cell towers that AT&T is using, but public safety will have priority, it will have pre-emption and it will have encryption. It will be a public safety network with a public safety applications ecosystem," he said.

The towers may be shared but the network will belong to first responders alone; a "distributed core" that is distinct from AT&T's commercial core network. "There will always be questions from folks," Kennedy said. "The easiest thing to do is to show them my prototype FirstNet device, where the network name is 'FirstNet.' When you see that on the device, it's easier to understand how it is going to work, that it is going to hit that cell tower and go to that secure network."

Emergency managers may feel tentative about sharing infrastructure, but economic realities make it a necessity. To create a network from the ground up "would take years to build, and public safety would have to wait a decade or more to have basic broadband service," LeGrande said. "What public safety needs and fought so hard for is priority and pre-emption."

That's what FirstNet is promising. Bratcher likes to use the analogy of a big concert or an NFL game. "Everyone is trying to use the network to upload photos and pictures and no one can get through," he said. "With FirstNet, there will not be any congestion. They will operate without any slowdown. The network knows you are a first responder and you get full access to that bandwidth."

What's opting out all about?

States and territories don't have to participate in FirstNet. Congress allowed an opt-out option for those that didn't want to join the network.

Kennedy said the opt-out has played a helpful role in FirstNet's development. The knowledge that state authorities could eventually decline FirstNet's offering has goaded planners, driving them to deliver the best possible product. "It was put in to ensure that we did the best job we possibly could," he said.

States that opt out still must build and operate their own broadband public safety network, albeit with limited federal funding. Some say it's an option worth exploring. With the right financing and a supportive vendor, "there could be alternatives out there that could implement that kind of model," LeGrande said. "States should evaluate all available options. This is a 25-year decision and states should not rush to judgment."

Though some may still choose this route, most experts have trouble making

the math work. "Each state needs to make its own determination about how things will get deployed, and how quickly they can get deployed," Ors said. "There may be a cost-benefit for opting out, but up to this point, I haven't seen any reason for it."

Lehr said opting out would likely hurt public safety across the board. "Congress made opting out very difficult for a reason," Ors said. "We don't want hundreds of separate networks not able to easily communicate no matter what the location or who responds. That's what we've endured for decades and it's proven to be ineffective."

What's the price for opting in?

As of this writing, 23 states and one territory (the U.S. Virgin Islands) had "opted in" to participate in FirstNet. What exactly does this entail? What do the states commit to when they opt in?

In fact, opting in commits the state to very little. State authorities effectively agree that they will consider FirstNet as their public safety broadband network when it goes live. As soon as the state opts in, AT&T is obliged to begin investing in infrastructure. FirstNet and AT&T bear responsibility for deploying, operating, maintaining and improving the network.

FirstNet touts the opt-in as being risk-free to the states. Iowa's press release at the time of its opt-in spelled out in detail all the things the state will not be responsible for, including "capital expenditures, operating costs and other costs like staffing, training, integration, environmental compliance and program management."

In fact, states don't even have to use the network, once it is built.

"There is no requirement for states cities and localities to subscribe their first responders," Lehr said. "Even if a state opts in, if the use fees and equipment costs are higher than what they are spending on commercial systems, there is the potential that the local governments won't subscribe their users."

States cannot mandate that local agencies sign up their users. If they don't fall in line, the whole FirstNet premise could become unstable: The financial model here only works if there are subscribers on the network. This may be another goad, another means by which FirstNet and AT&T are prompted to deliver an end product that satisfies not just the technical needs but also the financial constraints of the emergency response community.

"The choice to buy services is a local decision. Each agency makes the individual choice, so there is a lot of local control and local decision making," Kennedy said. "It's going to be up to FirstNet and AT&T to attract those public agency users."

Whether and to what extent local emergency agencies will sign up for the service, now that states have begun opting in, remains to be seen. Stay tuned — the saga continues.

Adam Stone is a contributing writer based in Annapolis, Md. adam.stone@newsroom42.com

PUBLISHER'S STATEMENT

Statement of Ownership, Management, and Circulation

(Required by 39 U.S.C. 3685)

Title of publication: Emergency Management. Publication No.: 5710. Date of filing October 1, 2017. Frequency of issue: Quarterly. No. of issues published annually: 4. Complete mailing address of known office of publication: 100 Blue Ravine Road, Folsom, CA 95630. Complete mailing address of general business offices of publisher: 100 Blue Ravine Road, Folsom, CA 95630. Full names and complete mailing addresses of publisher, editor and managing editor; Publisher: Alan Cox, 100 Blue Ravine Road, Folsom, CA 95630. Editor: Jim McKay, 100 Blue Ravine Road, Folsom CA 95630. Managing Editor: Miriam Jones: 100 Blue Ravine Road, Folsom, CA 95630. Owner: e.Republic, Inc. dba Government Technology: Dennis McKenna, Robert Graves, Cathilea Robinett, Alan Cox, Lisa Harney, Paul Harney, 100 Blue Ravine Road, Folsom, CA 95630. Known bondholders, mortgages and other security holders owning 1 percent or more of the total amount of bonds, mortgages or other securities, none.

Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
A. Total No. of copies (Net Press Run)	35,182	36,263
B. Legitimate Paid and/or Requested Copies		
1. Outside County Paid/Requested Mail Subscriptions Stated on PS Form 3541	23,076	25,939
2. In-County Paid/Requested Mail Subscriptions stated on Form PS 3541	0	0
3. Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution Outside USPS	0	0
4. Requested Copies Distributed by Other Mail Classes Through the USPS	0	0
C. Total Paid and/or Requested Circulation	23,076	25,939
D. Nonrequested Distribution		
1. Outside County Nonrequested Copies Stated on PS Form 3541	11,148	9,729
2. In-County Nonrequested Copies Stated on PS Form 3541	0	0
3. Nonrequested Copies Distributed Through the USPS by Other Classes of Mail	0	0
4. Nonrequested Copies Distributed Outside the Mail	30	0
E. Total Nonrequested Distribution	11,178	9,729
F. Total Distribution	34,254	35,668
G. Copies not Distributed	928	595
H. Total	35,182	36,263
I. Percent Paid and/or Requested Circulation	67.37%	72.72%
a. Requested and Paid Electronic Copies	5,971	5,808
b. Total Requested and Paid Print Copies + Requested/Paid Electronic Copies	29,047	31,747
c. Total Requested Copy Distribution + Requested/Paid Electronic Copies	40,225	41,476
d. Percent Paid and/or Requested Circulation (Both Print & Electronic Copies)	72.21%	76.54%

I certify that all information furnished on this form is true and complete.
Miriam Jones, Managing Editor

Storms P

Hurricanes reignite debates on flood control and the National Flood Insurance Program, and highlight the neighbor as first responder. **By Jim McKay**

APIMAGES.COM

our It On

Hurricane Harvey's real impact on Texas was the amount of rainfall it delivered.

Damage from Hurricane Harvey. Early estimates showed that as many as 130,000 homes were affected by the storm.

SHUTTERSTOCK.COM

Hurricane Harvey left in its wake more than 51 inches of rain and the distinction of being the biggest rainstorm in the history of the United States mainland, flooding a good portion of Southeast Texas in August and September. But right on the coattails of Harvey came Irma, battering Florida, and then Maria, all highly destructive events. At press time, recoveries from Harvey and Irma were underway and Maria had just leveled Puerto Rico.

The series raised issues like evacuation, flood insurance, climate change and flood control engineering — or the lack thereof — and showed just how responsive residents are and have to be when disasters occur. Nowhere was that more apparent, perhaps, than Texas, where neighbors, friends and relatives became, as they do in all such disasters, the "first" first responders.

Harvey Proves Again That Neighbors Are 'First' First Responders

More than 70,000 Southeast Texas residents needed rescue, and initially it was fellow residents who were there to help. Stories of the thousands of stranded Texas residents being aided or rescued by neighbors were numerous and illustrate the importance of being prepared and not relying on government first responders during the first hours of a disaster.

"There's no question that the residents of Harris County and other areas of Southeast Texas were among the very first to come to the rescue of their families, friends and neighbors during the Harvey response," said Harris County Judge Ed Emmett in an email. "I know of thousands of cases in which Texans from all over our area performed meaningful, selfless acts, ranging from boat rescues of strangers to stopping by to check on elderly neighbors."

Estimates were that approximately 30,000 residents needed shelter, and Emmett said that as of press time, the estimate of homes affected by Harvey was about 130,000. Although most residents had returned to their homes, many homes were destroyed.

Dun & Bradstreet crunched some early numbers and found that Harvey "potentially" impacted 561,830 businesses in Texas disaster-declared counties. In Florida, 845,702 businesses were "potentially" impacted by Hurricane Irma in disaster-declared counties.

Harvey prompted suggestions that Harris County planners were right decades ago when they said lesser storms could ruin a large part of Houston and its suburbs. Harris County Flood Control District engineers said that the area's reservoir system was insufficient and threatened thousands of properties.

Rain forced Addicks and Barker reservoirs to begin spilling water, exacerbating the flooding. Emmett called the storms "a new normal," and called for changes in the flood control system.

"I believe Harvey has shown us that we have to do more to mitigate the damage from these types of storms. But that will cost money, and we will definitely need a great deal of help from Congress and from our state Legislature," he said.

He said federal assistance is needed to shore up dams at Barker and Addicks reservoirs that protect downstream Houston from flooding, and perhaps build a third reservoir.

"We also likely will need to implement a major buyout program for many of the homes built in the floodplains behind those reservoirs and other flood-prone areas," he said. "And we need the Legislature to give us more authority to regulate development in those areas." He also called for a more regional reaction. "Flood waters don't confine themselves to county lines, why should our response?"

SHUTTERSTOCK.COM

What Made Harvey So Devastating? Is It the New Normal?

Emmett called Harvey more of a rain event than a hurricane and said that made it difficult to respond to and was one of the reasons evacuation wasn't considered.

"In a hurricane, you evacuate those in danger from storm surge and you generally know how much surge to expect and where it can be expected," he said. "In a rain event like Harvey, you can't really know in advance where the rain will fall and where the flooding will occur."

He said coordinated evacuation of millions in the area would have taken several days and that schools and businesses would have had to close well in advance of the storm. He said that in recent flooding events in Harris County, most deaths occurred when motorists were trapped in cars by rising water. Thus, it wouldn't be prudent to order people into their cars and onto the highways with such a storm moving in.

There are trends indicating that parts of the country, especially the Northeast and Midwest, are getting wetter. Kevin Trenberth, a senior scientist at the National Center for Atmospheric Research, said the air over the oceans is 5 to 10 percent moister now than pre-1970. He said that translates to 5 to 10 percent "heavier" rains or snows.

"But for hurricanes and some storms, it also intensifies the storm and potentially makes it bigger and longer lasting, which can easily double the affect," he wrote in an email.

Phil Klotzbach, research scientist in the Department of Atmospheric Science at Colorado State University, said in an email that Harvey wasn't anything that far out of the ordinary for Texas, but stalled after landfall.

"Unfortunately the storm stalled close enough to the Gulf of Mexico such that very heavy rain bands set up over the Houston metropolitan area, causing epic flooding," he wrote. "In terms of U.S. landfalling major hurricanes, there is no trend in these storms since the late 19th century."

The Dysfunctional Flood Insurance Program

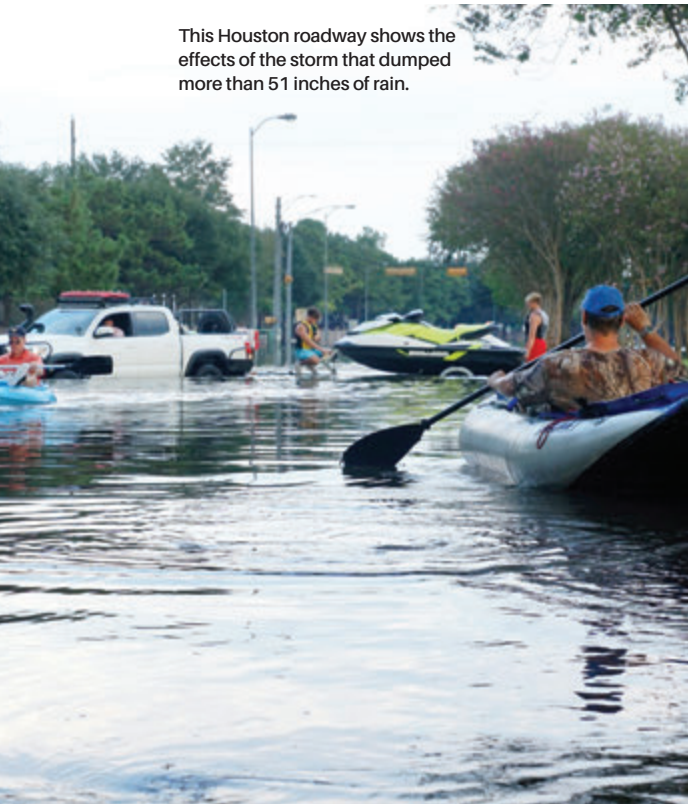
Harvey reignited flood insurance debate as well. Does the National Flood Insurance Program invite disasters such as Harvey by encouraging construction and rebuilding in flood-prone areas?

A report called *Higher Ground* by the National Wildlife Federation, showed that 2 percent of insured properties in the program were receiving 40 percent of the damage claims. Those are called repetitive loss properties — properties that file claims and rebuild after a disaster and repeat the process. More than half of the nation's repetitive loss properties are located in Houston, according to the report.

The National Flood Insurance Program is almost $25 billion in debt with no relief in sight. Chad Berginnis, executive director of the Association of State Floodplain Managers, told Bloomberg News that building homes just four feet above 100-year flood levels can cut insurance premiums by 75 percent, but that there is staunch opposition from the building industry.

There are currently tens of thousands of homes in the 100-year Houston flood plain, and Emmett said that the government should move as quickly as possible to begin buying out those in the flood plain. He said it's inevitable and will cost billions of dollars.

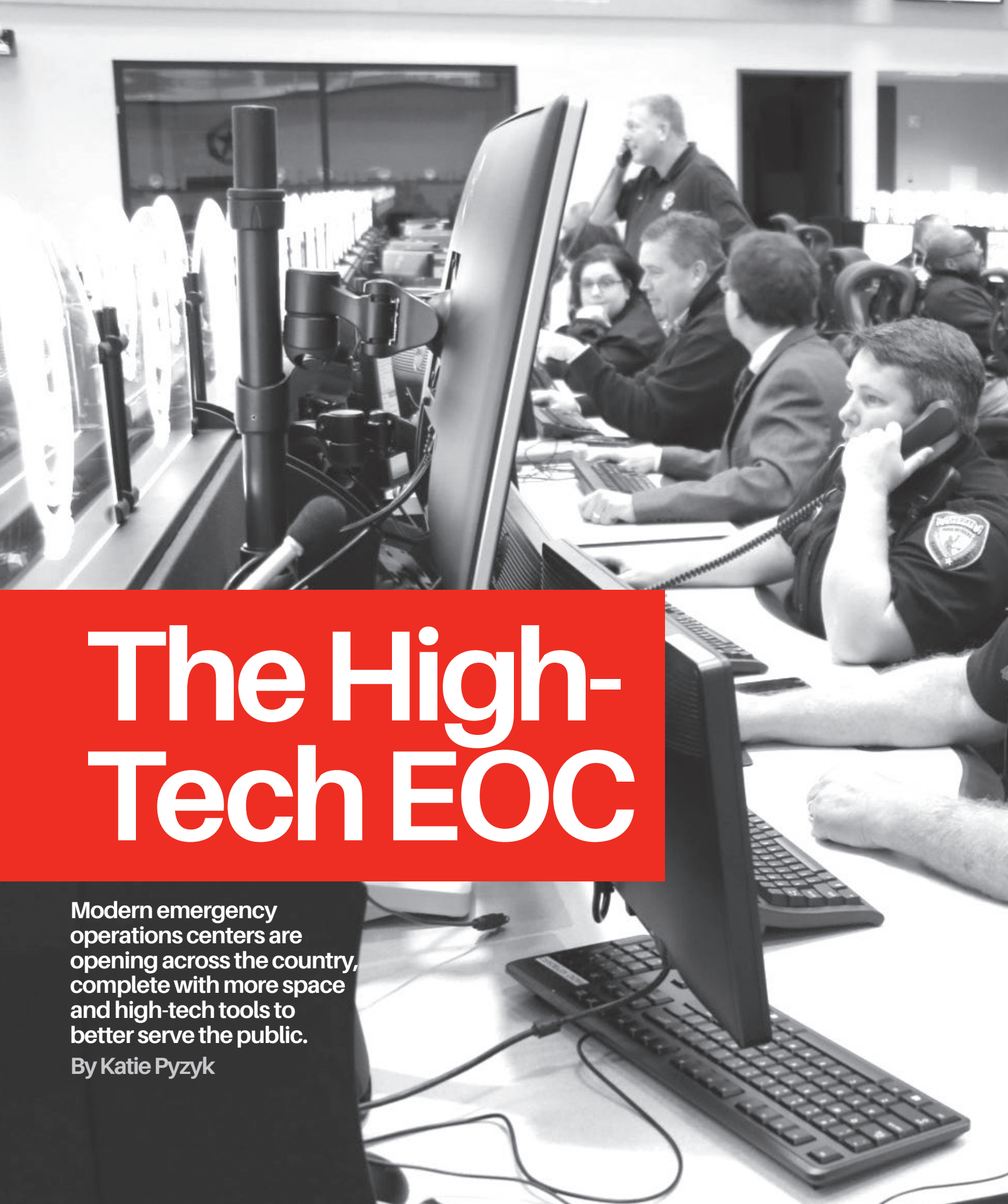
jmckay@emergencymgmt.com



This Houston roadway shows the effects of the storm that dumped more than 51 inches of rain.

SHUTTERSTOCK.COM

This aerial view shows Florida homes destroyed by Hurricane Irma.



The High-Tech EOC

Modern emergency operations centers are opening across the country, complete with more space and high-tech tools to better serve the public.

By Katie Pyzyk

Harris County, Texas, created a public safety campus. The 30,000-square-foot building accommodates several departments.

KATYNEWS.COM

Stepping inside an emergency operations center sometimes requires vying for a cramped spot in a bare-bones facility. But visiting one of the new, state-of-the-art emergency operations centers emerging across the country means encountering advanced technological tools situated in a more spacious environment. Safety professionals say these high-tech centers allow them to better assist the public in quickly navigating emergency situations.

Technology tends to draw the most attention, but it's generally not the primary factor driving the construction of a new EOC. Space constraints frequently motivate staff to campaign for a new facility. That was the case for New Jersey Transit safety employees, who had been working out of a 53-foot-long trailer for an EOC until they recently opened a permanent building.

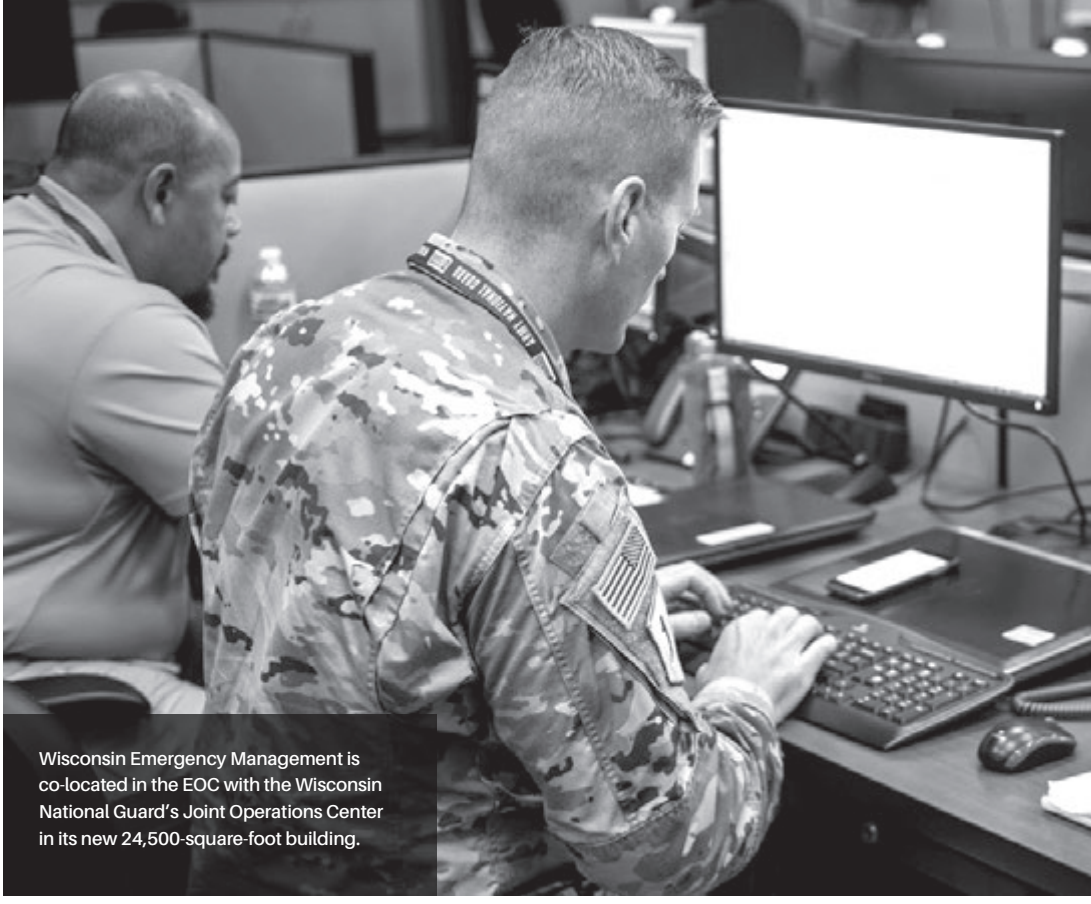
"It became very apparent that the facility we were using was not adequate," said New Jersey Transit Police Chief Christopher Trucillo. "It took a lot of coordination and convincing — because dollars are very dear in a public entity — to get folks to understand ... that we would be better at what we do as a result of having an adequately sized and staffed emergency operations center."

Wisconsin Emergency Management also struggled with functioning optimally in its previous facility because of "bottlenecks and large crowds and people crawling over each other," said Greg Engle, planning and preparedness bureau director. "It was very difficult for people to move around and work together. And we built some expansion capacity into [the new building] so if we have other agencies come in, we can set them up."

Insufficient space prompted emergency managers in St. Charles County, Mo., to request a new facility, which is scheduled to open next year. "We really need a more technologically advanced and bigger space to bring services to our residents," said Capt. Chris Hunt, director of emergency management. "The growth of the county and the responsibilities of public safety have increased tremendously."

Expanded emergency management responsibilities, in addition to the space issues, played a role in securing Wisconsin's new state EOC, which opened last December. "When I started 20 years ago, our focus was on tornadoes and flooding. But

emergency management has changed over the years to include [threats such as] 9/11 ... and cyberthreats," said Wisconsin Emergency Management crisis communications manager Lori Getter. "We have to continue to be ready to evolve and help our citizens."



Wisconsin Emergency Management is co-located in the EOC with the Wisconsin National Guard's Joint Operations Center in its new 24,500-square-foot building.

Many contemporary EOCs are anchored by a large main room that glows with dozens, or perhaps hundreds, of computer monitors located at staff work stations. Various room layouts exist, but most situate stations so workers face or easily can view a "smart wall," typically consisting of many smaller monitors or tiles. "We have a huge screen that can be a full screen or broken out into smaller screens or visuals," said Richard D. Flinn Jr., director of the Pennsylvania Emergency Management Agency.

New Jersey Transit finds its smart wall beneficial. "[It] enables us to integrate all our video, all our audio, all our networks and PCs, as well as commercial services like cable TV and satellite TV ... and put it up on the board," said Capt. Robert Noble, commanding officer for the office of emergency management. "And our 3,500-plus [closed circuit] TV camera system."

Cameras in public spaces, especially traffic cameras, have become a game-changing resource on which cutting-edge EOCs capitalize. The cameras offer real-time oversight of situational aspects. "If something happens, they zoom right in and see what's going on," Flinn said of employees at the Pennsylvania EOC, which opened last year. "That's something we did not have in the old building."

New Jersey Transit relies heavily on its video feeds to simultaneously observe a variety of conditions. "We can display up to 36 cameras on those monitors at once," said Noble. "Rail operations is using them to look at passenger flows or train movement, but we're also having the same set of eyes on noticing any terrorism action."

Although it's still rare, a few EOCs use streaming video transmitted by drones. "We're getting real-time images through drones or through state-owned aircraft," Getter said. The aerial images help officials to assess the scale of a situation, especially in areas that are difficult to access. The footage becomes more advantageous when used in conjunction with a geographical information system. "We've really pushed areas ... such as GIS," Getter said. "Using the traditional aircraft and drones for aerial footage ... and comparing them with the GIS mapping ... has been a tremendous asset. We're going to a whole other level."

Similarly, geocoding helps distribute messages to select groups of citizens via wireless emergency alert systems. "We are able to geocode" where an incident occurs and send an alert "right to [nearby citizens'] phones, and ask folks if they want to get information about what's happening," Flinn said. "Just keeping somebody informed about what's happening helps alleviate stress [and] it alleviates folks calling 911 to see what's going on."

Social media is another frequently upgraded area. "Social media has been the biggest addition to the EOC," Noble said. "We're able to quickly share a lot of information ... from people out in the field." Pennsylvania's state agency pushed social media to the forefront in its new facility as well. "We realized that in the changing world, we have to be involved in monitoring what's happening on social media," Flinn said.

High-tech tools fall short, however, without a solid technological infrastructure. Fast, disaster-resistant networks are another focus in new EOCs. "Our network infrastructure is going to be so robust and so powerful. We're not going to be limited by a network that is going to slow things down," St. Charles County's Hunt said. "And our county IT department is going to house all of their servers and all of their infrastructure in this facility."

That sharing of resources — such as space and technology — among departments and agencies is a financially beneficial trend prevalent at advanced EOCs. Wisconsin Emergency Management, for example, is co-located with the Wisconsin National Guard's Joint Operations Center in its new 24,500-square-foot building.

Harris County, Texas, essentially created a public safety campus. The 30,000-square-foot building accommodates several related departments, including emergency management and safety communications. "We made the best use of the building," said Judge Ed Emmett, director of homeland security and emergency management. "In our case ... it's the fact that you've got four different government entities sharing one building that makes it such an efficient use."

Pennsylvania's emergency management collaborates with the state Department of Transportation, whose employees "sit right

WISCONSIN EMERGENCY MANAGEMENT

beside our watch officers, 24/7," Flinn said. They also share space with some human services employees. Beyond cutting costs, such a system fosters relationships among groups that need to cooperate during an emergency. "We're working side-by-side on 'blue sky days' on planning and logistics issues, and then when an incident happens we have that relationship and flow right into activation mode," Flinn said.

In addition, agencies sharing space and viewing the same information on the EOC's smart wall speeds daily and emergency operations by eliminating the need to actively contact employees in other locations. "Information is presented in real time on the wall and everyone can make their own decisions based on the information that's in front of them," Noble said.

Safety professionals' increased roles and investments in capital-intensive tools both have led an increasing number of agencies to scrap the concept of using separate centers for daily operations and emergency activations. Instead, they occupy one well-equipped facility that allows for both. For example, many new EOCs include communications workers staffing a 911 call center, whereas that function is located separately from emergency management in many older configurations.

NEW JERSEY HIGHWAY PATROL

New Jersey Transit relies heavily on its video feeds to simultaneously observe a variety of conditions.

Emergency situations often unexpectedly require extended responses, but many existing EOCs are not adequately outfitted for longer-term operations. That, too, is changing in modern centers. "The whole thing has been designed for people to stay there for extended periods of time and work as efficiently as possible," Emmett said of Harris County's new facility.

During extended activations, emergency workers in under-equipped facilities might be forced to attempt to sleep in the midst of a bustling EOC. Managers realize the toll that takes on their staff, though, and modern EOCs therefore better meet basic needs. "What makes this of particular importance during an emergency is that you work in shifts," Emmett said. "For people who are ... not on shift, to be able to rest properly is a critical component."

Harris County's previous facility didn't have sleeping quarters and only had two showers. "To say it was not the most comfortable environment would be a real understatement," Emmett said. But the new building provides access to "two large rooms that can be converted to sleeping areas, about a dozen showers and locker rooms," he said. "We also made it easier to get food service in and out ... now we have loading docks, and those have improved things a great deal."

Designing the facilities to withstand natural disasters and security breaches further boosts value. The St. Charles County EOC, for example, will have few windows due to its location in a tornado-prone area. "It took about a year in working with constructors to develop an EF-5 rated building," Hunt said. Plus, it has "fencing and bollards ... it's all gated, all key card access. The entire campus is under video surveillance that's monitored 24 hours a day."

Most EOCs situate stations so workers face each other or easily can view a "smart wall," typically consisting of many smaller monitors or tiles.

PENNSYLVANIA EMERGENCY MANAGEMENT

Designing a new EOC doesn't simply involve hiring an architecture firm to figure out the details. Safety staff report taking an active role in offering ideas to improve upon their previous facilities by incorporating lessons learned from past successes and failures.

Harris County's staff carried over findings from Hurricane Rita because "that evacuation went very badly. ... One of the big problems was that people would get outside of Houston and they'd run into traffic jams in smaller towns," Emmett said. Therefore, the new EOC houses improved technology for monitoring traffic and communicating with responders assisting with traffic flow. "If there's an evacuation, I can monitor the traffic all the way to Dallas and San Antonio," Emmett said. "We can tell you the deputy that's supposed to be at each intersection monitoring it. If they don't check in on their laptop, we can find out why they're not there."

New Jersey Transit considered difficulties experienced during several longer responses when designing its new EOC. "The experience with Superstorm Sandy being so devastating and having an impact not just for a few days or a couple weeks, but literally for a couple months ... really crystallized the need to step up our game in terms of an emergency operations center," Trucillo said. Safety planning for the Super Bowl and the Pope's visit also were influential.

St. Charles County emergency management staff acutely felt their EOC's shortcomings when a tornado struck in 2013. "With all the emergency support functions [in there] it was extremely crowded and made it difficult to communicate," Hunt said. That prompted research into not just a larger space, but also noise and echo reduction measures to ease communication.

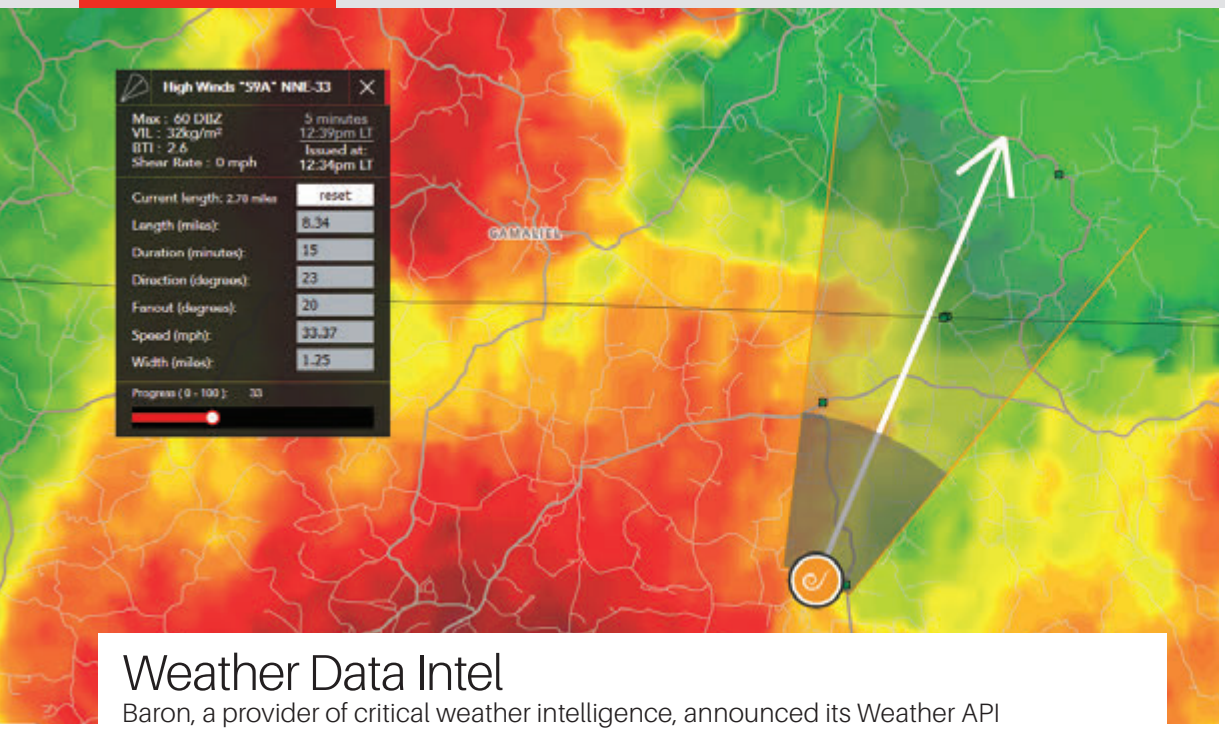
Agencies also benefit from researching other EOCs and learning from other entities. "Everybody should be doing that," New Jersey Transit's Noble said.

St. Charles County safety staff toured other new facilities and discovered the importance of right-sizing visual equipment in large rooms. Some EOCs they visited encountered problems from installing "what you think is a gigantic monitor on a wall. But when you put it up, it's really small. So you can't see what content is on those monitors," Hunt said.

Wisconsin Emergency Management staff visited and borrowed ideas from facilities in multiple states. Most notably, they reworked their main room's layout based on Ohio's EOC, "which groups together the different emergency support functions in pods," Engle said. "Our previous layout was in long rows like a movie theater. But in these pods people are working together more in groups."

Many agencies across the country have entered into new territory by constructing state-of-the art operations centers. But in the end, as Emmett said, "an EOC is only as good as the people that are in it."

slicesofpy@gmail.com



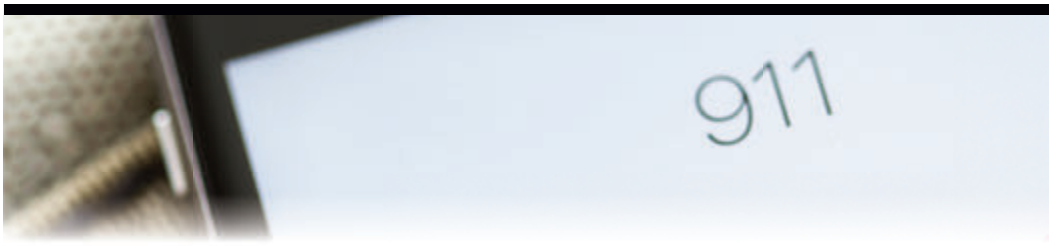
Weather Data Intel

Baron, a provider of critical weather intelligence, announced its Weather API (application programming interface) for Public Safety. This product is designed to make it easy to implement superior weather data into a variety of existing products and platforms that organizations use to track assets, equipment and staff to ensure effective public safety and emergency planning in all kinds of weather.

Baron's Weather API for Public Safety provides an accurate Internet-delivered meteorological data stream for turnkey integration into a range of devices and services. Timely and accurate storm tracking in Baron Weather API shows the current locations of severe weather, including hail, flooding, rain, high winds and tornadoes. Weather API for Public Safety also forecasts severe weather and gives an estimated time of arrival for the chosen community. All data in the Baron Weather API for Public Safety is provided in a variety of different formats with the developer able to determine how to present the information. **www.baronweather.com.**

SCALABLE ENCRYPTION KEYS

Internet Promise Group Inc. (IPG), a maker of security software, secure data storage and cybersecurity systems, has introduced Random Dance Keys (RDK), a new class of scalable encryption keys so virulent and ephemeral that they are impervious to brute force attacks. Unlike current data security methods that focus on creating more advanced encryption algorithms, RDK goes beyond the encryption key space itself that until now was the standard key size of 256 random sequences of bits. RDK encryption keys are engineered not only to be unbreakable by brute force methods, but also impossible to steal or hack by focusing on the innovation in the encryption key itself rather than the encryption algorithm. They are generated randomly for every data block within a secure communication channel, are unique per data packet, direction or time slice, and based on six layers of random separation for in-depth defense. www.internetpromisegroup.com



New Call-Handling Features

Airbus DS Communications announced added functionality in its VESTA 911 solution for next-generation 911 call handling. Three new features will allow public safety answering points (PSAPs) to decrease call-handling times, ease calltakers' workloads and lessen costs. These benefits translate to improved operations for enhanced focus on community safety.

Of the three new VESTA 911 features, two provide solutions to a growing problem within PSAPs nationwide — abandoned calls. These create additional work for calltakers who must manually return each call to determine if 911 assistance is necessary. The first feature is Automated Abandoned Callback and has the VESTA 911 system automatically return abandoned calls. It gives recipients the option to be directed to 911 dispatch for help or to report that they no longer need assistance. This removes the burden from calltakers to return each call.

The second feature addresses "pocket dial," a common culprit of abandoned calls accidentally made without the user's knowledge. To address the problem, Airbus is introducing technology that will detect voice or a button press on the dial pad to determine if a wireless call is a pocket dial or truly needs to be presented to a calltaker. If neither is detected, the call is considered a pocket call and is disconnected. **www.airbus-dscomm.com**

Big-Game Strategy

Niki Papazoglakis leads tech team to successful Super Bowl LI

Super Bowl LI was played in Houston in NRG Stadium Feb. 5, 2017. It was a boon for the city of Houston and Harris County and a potential nightmare for first responders. To make the event as safe as possible and to be as prepared as possible, Harris County prepared for about a year for the game and the 10-day event Super Bowl Live and NFL Experience leading up to it.

The preparation began at a rodeo, where first responders tested response, and continued leading up to the game with "dry runs" at Houston Texans football games and other events. At the heart of the preparation was Niki Papazoglakis, program coordinator for Harris County Information Technology and Services, who coordinated the public safety LTE network and mobile apps used during the events.

We snared Papazoglakis from her busy schedule to talk about the preparation and what was learned.

By Jim McKay | Editor

You started planning about a year prior to the Super Bowl. Tell me about the 30-day rodeo, what you did there and what you learned.

We deployed a variety of different kinds of devices. At the time, there were three versions of Band-14-capable hardware. The primary one we used was the Sonim Rugged Smartphone XP7, and we used a push-to-talk app and a location service situational awareness app for location tracking and broadcast messaging and picture sharing.

We went to the rodeo and said, "We have this technology and we'd like to use it, what are your communications problems?" They said they'd like to get nonemergency or nonessential traffic off their one security channel if possible, and they wanted a man-down feature. They didn't have location-identifying information on their radios.

We were successful in reducing the nonessential-type traffic, but it was a painful experience. Part of it was we didn't have our network built and were using a [Cell on Wheels] a half-mile away. But the main takeaway as we deployed was that it was

WIKIPEDIA

not really ready for boots-on-the-ground officers in a large-scale environment.

It worked well for them, but it was an isolated function. Since then, we've learned it works well for undercover teams and other types of use cases but not for a large-scale event. We came out of it thinking, "What now?" So we started from there with a blank sheet of paper.

We got buy-in from executive management from the Houston Police Department, Harris County Sheriff's Office and the Houston Fire Department to commit resources to figure out what we wanted to do with the whole premise of augmenting radio communication. And we said, "Who do we think the likely user groups were going to be?" It was the more specialized units. The field intelligence teams (FITs) had clearly the strongest use case along with special events and special response groups.

We brought them all together and asked what their problems were likely to be, and from there built requirements from the ground up.

Prior to bringing everybody together, we made a conscious decision to try to use tools that the city or county had already purchased and fill gaps as needed. We mapped requirements to the products we had available, and couldn't meet the majority of them.

> "We got buy-in from executive management … to commit resources to … the whole premise of augmenting radio communication."

We brought in an app called Moxtra as a group messaging and collaboration platform. We tabled some of the other tools when the users saw this one. The majority of our use case was around data-augmenting radio communications.

Tell me about the dry runs, how many of them there were and some of the experiences you had.

We had several. We used every home Texans game and other events like the Houston Marathon and the Thanksgiving Parade, stuff like that. People think Super Bowl and they think Game Day, but from a security standpoint, the broader threat was probably at the George R. Brown Convention Center, which was a 10-day event Super Bowl Live and NFL Experience. The bulk of the planning revolved around Super Bowl Live.

The Texans games proved not incredibly valuable to us in developing the Concept of Operations and the standard operating procedures because the officers that provide security are extra. It's not their regular job, and they don't have the same type of mentality, and it's not the same kind of command and control structure in place.

The FIT sent two teams every week to go into the fusion center every home game and practice and test the technology. The games worked well for the EMS folks because they loved the ability to do the messaging.

We learned a lot at the Thanksgiving Parade in realizing who should have the technology and where it should be placed. The fire department got a lot of value out of using the location tracking to quickly dispatch their bike teams to medic calls and things like that.

It culminated with the marathon, and the biggest thing we learned from this is we had everyone in one chat room and that was great information for certain teams but created a lot of unnecessary notifications for everyone else. Like the bomb tech would get dispatched for a suspicious package and would take a picture of it but the other users didn't care about that information. The biggest takeaway was we needed to segregate the teams and come up with an information flow of how the information would move from team to team and be shared.

You said that text messaging and picture sharing were the keys. Talk about the significance of that.

It so far exceeded our expectations of how it would be used and how successful it would be. The radio traffic between the city and county systems only went up 10 percent during that 10-day operational period. The messaging app was viewed almost 60,000 times and there were almost 7,000 unique messages created and like 1,200 pictures and videos so it was really heavy use. A lot of it was not the sexy stuff like arrests, but it was a lot of logistics. For example, an officer at a hotel took a picture of a printed list of license plates and sent it out saying these are the governor's vehicles and are going to be parked here. That eliminated all the radio traffic of people calling in plates asking questions about the vehicles.

The pictures were incredibly valuable because it just cut down on the voice descriptions of things and the confusion and asking of questions and clarifications. It also significantly improved the information-sharing and interoperability across teams.

By Eric Holdeman

A Climate Heart Attack

There are many people who ignore reality every day. You know them; they are your co-workers, your relatives, your friends and perhaps even you. These are people enjoying life, with established bad habits. They eat and drink what they want; smoke what they want; chew what they want; and believe that a day without exercise is a day without pain.

Sometimes we refer to them as ticking time bombs or walking heart attacks just waiting to happen — but, they haven't. Therefore, they continue on their merry way, living life how they have perhaps done so for 20, 30, even 40 years with no observable consequences. And we all know someone who smoked until they were 90 and was healthy as a horse.

But — and it is a big but — those behaviors will eventually catch up with 99.9 percent of the population who do not live to be 90 having never given a thought to their habits. My own father was one of those people. A two-pack-a-day Camel smoker for most of his life — he died of a heart attack at age 54.

My father died in 1977, before they had all the diagnostic tools available today. There were no treadmill stress tests or angiograms. He did not have a chance to change his behavior after the heart attack.

The question I have for you is this: Are the twin disasters of hurricanes Harvey and Irma sufficient in their impacts to cause people and organizations to rethink the climate heart attack that we just collectively experienced?

The behaviors that have led to these events have less to do with carbon and more with climate adaptation. States, counties and cities continue to promote development in areas susceptible to disaster impacts. Building homes, resorts and commercial structures is a major contributor to the economy of these governments. They provide a continuous stream of growth in the form of jobs that surround the construction industry.

What might the "climate doctor" tell us to do to avoid having a "climate heart attack"? I can expect the list of recommendations might include:

- Rethink your zoning laws and look to establish broad swaths of green space in the form of parks or golf courses that might flood, but won't impact homes, businesses and critical infrastructure.

- Institute building codes that add to the disaster resilience of the structures as they are built or rebuilt. Cheap has its benefits, but better will last longer and protect families and businesses from economic catastrophes that destroy families and livelihoods. My sister's home in Naples, Fla., built to hurricane codes, experienced 140-mph winds with no structural damage to the home itself.

Unfortunately, in some jurisdictions, it may require establishing building codes where none exist today.

Emergency management's role in climate issues has to do with "climate adaptation." Others will focus on causation of warming global temperatures. I'm not negating the need to do this, but professionally we need to be "adaptation therapists" — helping people get back on their feet, but doing it in a manner that will prevent future injuries.

One of my favorite quotes is, "The lessons will continue to be taught until they are learned." As I write this on Sept. 18, 2017, there are a couple of other hurricanes — lessons — spinning counterclockwise in the Atlantic Ocean. Will it require another climate heart attack to change?

Eric Holdeman is the former director of the king County, Wash., Office of Emergency Management. His blog is located at **www.disaster-zone.com**.

By Larissa Paschyn

CERT Should Be Mandatory

Too often, businesses and organizations rely on the hope that first responders will be able to reach them in time during a major disaster. However, the bigger the disaster, the more strain on limited resources, and the less likely the government will be able to respond. As a result, it is imperative that everyone in an organization can use their own resources and skills to take care of each other.

FEMA maintains the Community Emergency Response Team (CERT) program as an official emergency preparedness program. However, there is no obligation or requirement for schools and employers in high-hazard areas to implement or maintain such programs on site.

The CERT concept was originally developed following a series of earthquakes in the U.S. and Puerto Rico that left hundreds dead, injured and without emergency services. CERT volunteers are educated about disaster preparedness for the hazards that may impact their area, and CERT trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization and disaster medical operations. Local responders can rely on CERTs during disaster situations, which allows them to focus on more complex tasks.

Yet public education campaigns encouraging participation in CERTs have not been highly effective or visible. For example, in California's Bay Area, few residents are even aware that their neighborhoods offer CERT. Combine that with the fact that numerous IT companies in the Bay Area are basically small cities, and you are looking at a recipe for disaster. With the limited manpower and resources local emergency response has, these IT villages are not likely to receive help for a long period of time. And let's not forget the sheer density of downtown San Francisco and Oakland, where emergency response will also have a difficult time responding to all affected buildings.

Without holding schools and businesses accountable, there is a greater likelihood of loss of life when a catastrophic disaster occurs, such as tornado, flood or earthquake. In a catastrophic disaster, first responders will not be able to assist for a prolonged period of time. By requiring businesses of more than 150 persons and schools to have a work or campus-based (C-CERT) team in place, local public safety can focus on other areas [during an emergency situation]; allowing the affected school/company to be self-sufficient for a time.

In any disaster, you can find numerous accounts of neighbors and regular citizens assisting at the scene before response agencies could deploy. After the Joplin, Mo., tornado in 2011, neighbors assisted in digging others out of the rubble. During the 2016 Louisiana floods, instead of waiting for the government to come rescue them, the people of Louisiana used privately owned boats to save their neighbors. This "Cajun Navy" was responsible for saving the lives of thousands of Louisianans.

In South San Francisco, biotech companies have been ahead of the game for years, maintaining on-site search and rescue, medical, hazmat teams, and incident command teams. In the event of an earthquake, they will be able to rescue and treat their own staff before help arrives.

The fact is that our communities and our facilities are one of the most effective ways to ensure that we are prepared in the event of a future emergency response situation, and every business should be a part of that preparedness. Schools and companies need to be able to take care of their own people, and in earthquake territory, it is irresponsible not to require all corporations and educational institutions to have response programs in place.

Larissa Paschyn is the emergency manager for Amgen in South San Francisco, where she trains the emergency response teams. Previously, she was the external affairs officer for the FEMA Region 9 Incident Management Assistance Team.

One Unified Solution

for all your incident management needs

Visual Situational Awareness

Emergency Communication

Tracking and Reporting

Fully Customizable

Task, Mission, and Resource Management

Don't waste your time and money with disjointed dashboards or multiple solutions. DLAN provides everything your team needs to prepare for, respond to, and report on issues - anytime, anywhere, from any device – all in one easy to use system.

Call 716-822-8668 or visit DisasterLAN.com to get your free demo today!

DLAN

DLAN shown on Bak USA's Seal Rugged Tablet. Apple's iMac, and Apple's iPhone. Apple, the Apple logo, iMac, and iPhone are trademarks of Apple Inc.