Vol. 37 No. 6 June 2020

INTERNATIONAL ASSOCIATION OF EMERGENCY MANAGERS

IAEM Bulletin

In this issue

IAEM Deadlines

- **IAEM Awards Entry Deadline: 5 p.m. EDT, June 30 > p 7**
- **IAEM-USA Officer Nominations Deadline: 5 p.m. EDT, July 2 > p 9**
- **Scholarship Applications Due: 11:59:59 p.m. CDT, July 15 > p 15**
- **Call for Bulletin Articles on 'Crumbling Infrastructure' Deadline: July 20 > p 18**
- **Scholarship Commission Nominations Deadline: July 31 > p 16**
- **Certification Commission Nominations Period Ends: Aug. 1 > p 12**

IAEM-USA Diversity Committee Issues Open Letter to Emergency Managers

June 12, 2020

Emergency Managers:

Over the last couple of weeks, we've witnessed an outpouring of support worldwide from diverse populations standing up to racial injustice and privilege. Several companies, organizations and agencies have sent out correspondence supporting the cause that Black Lives Matter and speaking out against the horrible images of the death of George Floyd. Some were better than others, some had good intentions, while some addressed the countless others who lost their lives at the hands of others.

Hopefully, each of us has taken some time to reflect about the recent events and how they impact us as individuals, impact our co-workers in the agencies where we work, the communities we live in, and our profession as emergency managers. This may have caused some of you to initiate or engage in conversations to understand this isn't a new movement – that it's not rooted in the events that have occurred over the last few weeks in Georgia, Kentucky and other places that haven't made the news.

Let us not forget that all of this is occurring amid a public health crisis that has claimed thousands of lives – one whose rate of infections and deaths continues to disproportionately impact black and brown communities across the country. Sadly, this has led to discriminatory practices and actions against our Asian American neighbors and communities.

As emergency managers, some of us had to activate our emergency operations centers to respond to local events, but most likely not addressing how the activities in our communities may be impacting those we work shoulder to shoulder with every day. We have a job to do – to respond to our communities' needs and, in some cases, to help restore and recover – but we cannot do this effectively if we don't understand

continued on page 2

Leslie Luke Named IAEM-USA Diversity and Equity Advisor

IAEM-USA President Teri Smith, CEM, CPM, appointed Leslie Luke, deputy director of the Los Angeles County Executive Office, Office of Emergency Management, as the IAEM-USA diversity and equity advisor. The IAEM-USA Board approved the appointment at its meeting on June 16, 2020. Mr. Luke is the current chair of the IAEM-USA Diversity Committee, which formed in 2011. See press release.

"Today's decision by the board to add a diversity and equity advisor demonstrates the board's commitment to making their processes, discussions and decision-making more inclusive, open and representative of the membership," said Mr. Luke. "Strategically and operationally a board that is open to change and embraces diversity leads from a position of strength and sets itself up for future success and growth." ▲

201 Park Washington Court, Falls Church, VA 22046-4527
phone: 703-538-1795 • fax: 703-241-5603 • info@iaem.com • www.iaem.org

June 2020 Feature Articles

Special Focus Issue: "Black Swan Events – Cybersecurity"

IAEM Bulletin Advertising

Obtain details on ad guidelines and costs at www.iaem.org/Bulletin.

IAEM members and EMEX exhibitors receive a discount on advertising.

Questions? Contact Karen Thompson, editor.

The *IAEM Bulletin* is distributed monthly to the 5,000+ members of IAEM, plus others with government and legislative roles in emergency management. It is distributed at national, regional and state emergency management conferences. The specialists who read the *IAEM Bulletin* frequently play a key role in selecting, purchasing, and using emergency equipment, supplies, products and services. ▲

The IAEM Bulletin, which is a benefit of IAEM membership, is in its 37th year of providing information, resources, and ideas for IAEM members. Invite your colleagues to check out the free sample issue on "Black Swan Events: Pandemics" (April 2020) at www.iaem.org/Bulletin.

Call for Articles for the August 2020 IAEM Bulletin

Article Deadline: July 20, 2020

Special Focus Issue on "Black Swan Events: Crumbling Infrastructure"

Many of us are facing the challenges of crumbling infrastructure, including power grid failure, weakened dams and bridges, and general aging of the infrastructure as a whole. How do emergency managers prepare their communities when the potential disaster has not yet occurred? Share your experiences in an article for this issue. What did you and your community learn from an event that occurred due to crumbling infrastructure? It is more obvious than ever that our world is rapidly changing. How will we learn to operate in an environment that is unlike anything in our past? Will technology be our friend or an obstacle? Where are the opportunities for growth, development, change and synergy as we move into the future world of emergency management?

The IAEM Editorial Committee is seeking articles on the subject of "Black Swan Events: Crumbling Infrastructure." Article length is 750 to 1,500 words. Please read the author's guidelines if you have not previously submitted an article or if you are not familiar with the IAEM Bulletin. Article submission deadline is May 20, 2020.

To find out about additional future special focus issues, visit the IAEM Bulletin web page. Remember, the Bulletin is a monthly publication. Articles are sought on a wide variety of topics of interest to EM professionals for the issues that are not special focus issues. The Editorial Committee will continue to consider articles about the COVID-19 pandemic. ▲

Cybersecurity in COOP/COG: The "New" Normal

By Michael Prasad, CEM

Emergency management, other government departments and agencies, and private entities are types of organizations whose Continuity of Operations Planning (COOP) and Continuity of Government (COG) missions can be severely impacted by Black Swan Events/pandemic incidents. And for those organizations that have day-to-day disaster cycle missions (preparedness, response, recovery and mitigation), those emergency managers will most likely be performing "double duty." This can include the responsibility for restoring and supporting day-to-day operations of their organization *at the same time* as they are managing their pandemic missions.

What is new for many emergency managers, for this type of incident, is the significant social distancing public health response and its **massive all-at-once** switch to virtual meetings, communications and heavy reliance on technology and systems. The pandemic has effectively forced the organization into COOP/COG mode. One barometer of this effect was the significant increase in the personal use of web conferencing services, as evidenced by a multi-fold increase in downloads of those smartphone apps shown in the graphic below.

The reliance on technology to perform normal and pandemic operations, such as virtual staffing of an Emergency Operations Center or holding a "Planning P" web conference, will expose organizations to an increased risk for cyber-attacks, espionage and data theft. All organizations should have cybersecurity policies and procedures for their workforce, partners, and suppliers for their operations on a normal basis. Those elements also should be included in their COOP/COG plans.

Role of DHS/CISA

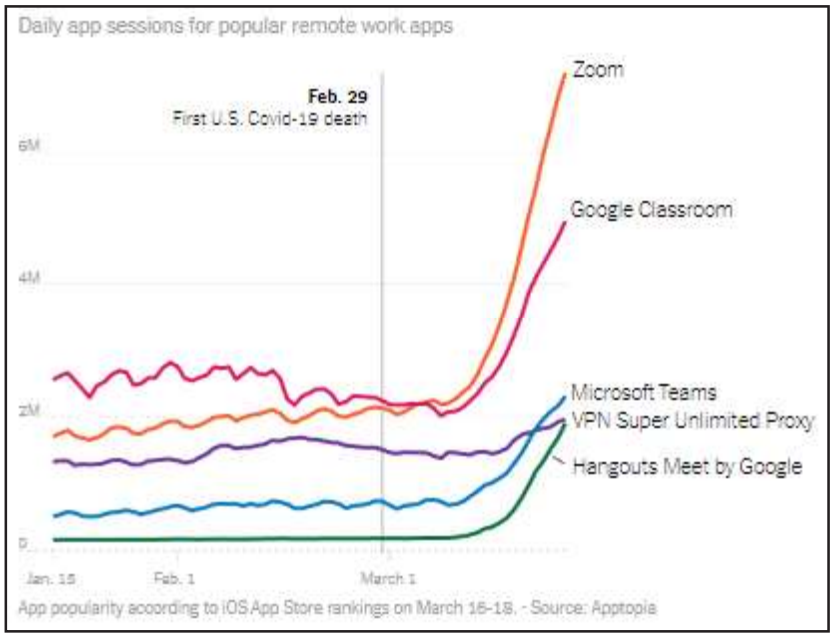
The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is now the umbrella federal organization for the U.S. Computer Emergency Readiness Team (US-CERT) and the National Cybersecurity and Communications Integration Center (NCCIC). CISA's sub-agencies and groups are a hub of information, alerts and expertise for cybersecurity and communica-tions information.

Recognizing that cyber threats will increase during Black Swan Events is paramount. Bad actors will take advantage of vulnerabilities and add layers upon layers of threats and risks, as far and wide as they are allowed. Planning for those attacks includes subscribing to and monitoring alerts from CISA. Any potential espionage and/or data theft is no different during a pandemic, but the cyber impact will be greater due to the COOP/COG state of the organization.

New Threats and Risks

Here are just some of the new threats/risks:

- **Zoombombing** is a situation where uninvited attendees break into and disrupt online meetings or conferences, often with hate-filled or other malicious content.
- **Advanced Persistent Threat (APT) groups**, a subset of malicious cyber actors, are targeting individuals, enterprises and organizations, sometimes masking themselves as trusted entities. Cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware. These attacks can be crippling to an organization in a virtual environment, in that there may be no alternative resources (backup facilities to work directly together, available non-infected computer devices, etc.) nor onsite tech support to correct.



continued on page 26

Cyber-Attack – What Happens Afterward?

continued from page 24

This data either validated the current computer security training or further identified what gaps needed to be addressed.

Summary

This type of follow-up should take place after any all-hazards incident, whether it is through multiple debriefings or a formal detailed after action report (with an improvement plan). An incident's individual characteristics may change. These incidents may dictate changes in policies, procedures or checklists. Ensuring that those changes are documented is necessary to help the next group of responders be better prepared for what is to come. Yes, it may be an uncomfortable experience, especially when every one of your policies and procedures are questioned and require justification. But it is one of those requisite processes that everyone must go through in order protect their agency's operations, functions and well-being. This applies not only to government entities but also to the private sector. ▲

Cybersecurity in COOP/COG: The "New" Normal

continued from page 25

■ The workforce was not prepared to fully telecommute, and the U.S. supply chain was not ready for the increased demand for computers and peripherals. Many home computers now double as the school, cookbook, logistics ordering system, and now office – sometimes with conflicting schedules.

Home networks, and the broadband network systems to which they are connected, are being overloaded with streaming videos. Missing or broken equipment, including a huge worldwide increase in the demand for web cameras, can degrade workforce capability at home.

Many broadband networks were designed with different upload speeds than download speeds (more aligned with streaming video into the home, than uploading mega data or interactive video-conferencing). Fine-tuning is a challenge during normal times; during a complex coordinated attack and a pandemic, it moves way up the consequence management planning scale.

■ **The reliance on cellular networks** – even the grand promises of FirstNet from AT&T – for COOP/COG operations – while a reasonable contingency for traditional COOP/COG operations to have as a backup/alternative for traditional wired internet service provider (ISP) connectivity – are a partial solution at best. The bandwidth for cellular data transmission (download speeds and even more impactful upload speeds) is significantly less than coax or fiber ISP connections. Major telecom companies indicate they are building more cell sites, increasing use of fiber optics in their network and upgrading routing/switching equipment. This will add capacity over time, but none of it will reduce the impact of a cyber attack on their systems. There is no single panacea for technology failures, especially communications systems. If your landline system is compromised by a virus, you can switch to cellular (and maybe GETS/WPS). If that fails (or worse – that network system is still partially working, where everyone does not have a clear indication that the entire network needs to be bypassed), you can switch to satellite or FirstNet. This means switching to a different channel on the same network of existing towers and switches, unless your organization has the capability to request and receive additional equipment). If a critical app is compromised on a networked computer or smartphone due to a malware virus or a communication network's switch is brought down by a distributed denial-of-service (DDoS) attack, COOP/COG is still impacted.

Next Steps

Looking for next steps to see where your organization stands? FEMA has a Pandemic Influenza Template to assist organizations with their Continuity of Operations Plan as well as two free online courses (IS-520: Introduction to Continuity of Operations Planning for Pandemic Influenzas and IS-522: Exercising Continuity Plans for Pandemics), which anyone can complete. From a consequence management perspective, imbedding pandemic planning – and particularly the cybersecurity impacts of social distancing/working remotely for continued operations *and* COOP/COG operations – should become standardized in this "new" normal of a post-COVID-19 world. Now is also the time to be **vigilant** and exercise those consequence management plans (the "what ifs" for your organization's COOP/COG planning as well as your day-to-day operations), as they relate to both a reduction in work force (including the absence of key leaders – one of the prime pillars of COOP planning) and a simultaneous cybersecurity incident. ▲