EMR-ISAC
Emergency Management & Response-Information Sharing & Analysis Center

The InfoGram

Volume 16 – Issue 8 *February 25, 2016*

Highlights:

Disclaimer of Endorsement:
The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.

The U.S. Fire Administration maintains the **Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC)**.

For information regarding the EMR-ISAC visit **www.usfa.dhs.gov/emr-isac** or contact the EMR-ISAC office at: **(301) 447-1325 and/or emr-isac@fema.dhs.gov.**

Hospital Hit with Ransomware Attacks

A California hospital recently paid hackers $17,000 to stop a ransomware attack that locked the hospital's computers and network. Federal and state law enforcement are still investigating, but as the ransom was paid via an internet currency, it is very difficult to trace who collected the money. In addition, because this particular ransomware attack was successful it may prompt more attacks against hospitals.

It is important to note the hospital's networks were affected and shut down for over a week, and the ransom in this case was 40 bitcoins, quite a bit higher than the usual 1-2, likely due to the significant value placed on medical records and care. The ransomware "industry" may bring in nearly $1 billion per year.

Hollywood Presbyterian Medical Center did not let this attack hinder their patient care much. They reverted to paper patient records and registration, and diverted some emergency patients to other hospitals. They state there is no evidence patient records were accessed or tampered with during that time.

This is the first known ransomware attack on a hospital, though law enforcement agencies have seen such attacks in recent years. It is likely not the last to hit a hospital and with this success, hackers may branch out into other formerly hands-off fields. Now is a good time to reevaluate your organization or agency back up systems. Back up records on a regular schedule and store the backup offline. Also, educate employees about malware links in emails, which may what initiated this attack.

(Source: FBI)

Cybersecurity Webinar for Health and Public Safety

The first Critical Infrastructure Cyber Community ($C^{3)}$ Voluntary Program webinar of 2016 will focus on the sectors related to health and safety, specifically Emergency Services, Healthcare and Public Health, and Food and Agriculture. Join the webinar to learn how these sectors are integrating cybersecurity measures, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, into their comprehensive enterprise risk management.

- Thursday, March 3, 2016, 1:00-2:30 p.m. Eastern
- Dial-In**:** 1-888-455-9681
- PIN: 5853466

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

Please RSVP to CCubedVP@hq.dhs.gov, or contact them if you are interested in learning more about the C3 Voluntary Program webinar series or would like to participate in a webinar.

(Source: C3 Voluntary Program)

A Look at 2015 Derailment Response in Philadelphia

In May 2015, an Amtrak train derailed at a high rate of speed in Philadelphia, injuring more than 200 passengers and crew and killing seven. Victims were treated at several local hospitals, including Temple University Hospital.

The inaugural issue of The Exchange (PDF, 6.9 Mb), the newsletter from the U.S. Department of Health and Human Services' Technical Resources, Assistance Center and Information Exchange (TRACIE), talked with Temple University Hospital's Physician Medical Director about their response to the incident, including lessons learned that can be applied to hospital response as well as EMS, law enforcement, and fire:

- While EMS transport of patients was logged, police transport was "invisible," un-triaged, and caused issues with patient tracking and overload;
- Staff made room by moving non-critical patients to other hospital areas;
- The hospital normally uses electronic recordkeeping; relying on paper registration during the crisis caused problems tracking and recording patients, their records, and tests;
- The area set aside as a family support center lacked the needed phone lines and computers and, again, patient tracking became an issue;
- Off-duty staff called to ask if they were needed instead of just showing up. This relieved crowding and ensured proper staffing levels the next day.

The hospital official credits its all-hazards approach to crisis planning as being critical, since they had worked through the processes many times before, if at a smaller scale. These lessons learned can assist other facilities in their crisis planning.

(Source: HHS TRACIE)

UAV/Drone Webinar: Hovering Friends or Foes?

An upcoming three-part webinar series on Unmanned Aerial Vehicles (UAV)/Drone technology will help agencies and organizations looking to better understand and handle the issue of UAV/Drones. Topics include the variety of UAV types and their capabilities; operational uses; current policy; training and exercises; how to improve UAV/Drone-related incident response; and current capabilities on disabling them.

- Webinar #1 - March 3, 2016, 1 p.m. to 2 p.m. Eastern
  Topic: UAV/Drone Technology Overview
- Webinar #2 - March 10, 2016, 1 p.m. to 2 p.m. Eastern
  Topic: UAV/Drone Use Cases, Threats and Deterrents
- Webinar #3 - March 17, 2016, 1 p.m. to 2 p.m. Eastern
  Topic: UAV/Drone Policy, Barriers and Recommendations

Those interested in attending must pre-register. This webinar is being organized by the Regional Consortium Coordinating Council (RCCC), the All Hazards Consortium's Multi-State Fleet Response Working Group, the U.S. Department of Homeland Security's JCIP (Joint Critical Infrastructure Partnership), and several other organizations.

(Source: RCCC)

Fair Use Notice:

This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local *FBI office* and also the *State or Major Urban Area Fusion Center*.

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201**, or by email at **nicc@dhs.gov**.