Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 18 — Issue 43 | October 25, 2018

Firefighters again targeted in shooting on fireground

A gunman ambushed firefighters and shot at them in Oregon last week, adding another incident to the growing lists of both ambush attacks on first responders and firefighters being targeted by violence.

This incident is very similar to the deadly 2012 Webster, New York shooting: a man sets his house on fire, then waits for first responders intending to shoot them. In the Oregon incident, however, no one was injured. One bullet went through the pants cuff of a firefighter, and several bullets hit a fire engine windshield.

There are growing reported threats toward law enforcement officers nationwide, and ambush attacks remain high as well. All public safety and first responder personnel must take every precaution at active crime scenes, fires, medical emergencies, accidents and all other incidents. An assailant may target people on the scene just because they are wearing a uniform.

It is crucial to maintain situational awareness at every incident, and all first responders should know the difference between cover and concealment. Complacency in seemingly innocent, routine situations can mean not going home at the end of a shift.

(Source: FireRescue1)

Two ransomware attacks against local government end differently

Last week a water utility in North Carolina and a town in Connecticut were both hit with ransomware attacks. Both had their systems crypto-locked, and in both cases the attackers demanded a cryptocurrency payment. But the end results of each case were different.

The North Carolina public water and sewer utility services a population of 100,000. It believes this was a targeted attack, falling just after Hurricane Florence. The utility decided to ignore the ransom demand of $23,000 and will instead rebuild the system and restore data from the backup files.

One reason it decided not to pay the attackers, which they confirmed were in Iran or Ukraine, was because the ransom money may very well be funding criminal or terrorist activities.

The Connecticut town affected did pay the ransom, though in its case it was much less at $2,000. This attack was also traced overseas. Local police worked with the Multi State-Information Sharing and Analysis Center (MS-ISAC), who specializes in helping state, local, tribal and territorial governments with cyber-related issues, and determined paying was the best option.

Advice varies about whether or not to pay ransoms, and the FBI recommends not paying. There are many variables in the decision and while “giving in” to an attack like this is unsavory, stories like Atlanta’s $3 million+ ransomware clean-up costs are shocking. Atlanta elected not to pay a $57,000 ransom this past spring.

It is crucial that your town, department, agency or office have up-to-date network security software, institute a regular data back up system and that your backed-up data is stored separate from the network. These steps are a good beginning toward

Highlights

U.S. Fire Administration

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

setting up a cybersecure system.

(Source: HealthCareInfoSecurity.com)

Responding to improper use of Unmanned Aerial Systems

Improper or illegal use of Unmanned Aerial System (UAS) challenges law enforcement investigations, but the new video "Safer Skies: How the FAA Helps Law Enforcement Respond to Reports of Improper Use of UAS" gives a crash course in steps departments can take when these cases crop up.

This new video from the Justice Technology Information Center (JTIC) serves as an introduction to the Federal Aviation Administration's (FAA) role in UAS-related criminal investigations and FAA resources for law enforcement agencies.

The FAA estimates over a million UAS pilots are operating within United States air space, so it is likely your department will encounter this issue eventually.

Most drone-related violations are likely to fall under established local or state laws such as voyeurism, trespassing, state aviation laws or obstruction of justice. See the FAA's UAS Law Enforcement and Public Safety website for more detailed information on handling UAS reports.

(Source: JTIC)

Next Generation 911 cost study project

911 funding models have not kept pace with changing technology in recent years. As emergency communications moved through cellular and Voice over Internet Protocol (VoIP), and now the push toward Next Generation 911 (NG911), figuring out how to pay for it continues to challenge governments responsible for implementation.

Congress directed a study to assess the service requirement and specifications to implement NG911 across the country and the associated costs. The results were published earlier this month in the "Next Generation 911 Cost Estimate Report," (PDF, 5.74 MB).

The report is detailed, ultimately analyzing three major implementation scenarios:

- Individual state implementation - independent states/territories purchase, implement and operate a NG911 solution with a minimum of two centers.
- Multistate implementation - multiple states/territories within 10 geographical areas coordinate toward a shared solution.
- Service solution - independent states/territories purchase all core services and PSAP system maintenance from a NG911 service provider.

Each scenario assumes a 10-year implementation period and takes into account things involving system design and set-up, governance, maintenance and personnel training. The information presented in this report can assist your region to better implement NG911 and anticipate the associated costs.

(Source: 911.gov)

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.

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.

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.**