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

Highlights:

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.**

The InfoGram

Volume 16 – Issue 39 *September 29, 2016*

Protecting Your Digital Footprint

The amount and types of personal information and photos we have become used to seeing and posting online should be enough to make you cringe when you stop and really think about it. If someone could get access to all of it, they could have a level of access to us – and our families – unheard of even 10 years ago.

The problem is, this is happening to first responders, public servants, and military members across the country as hactivists and terrorist-sponsored hackers gain access to social media sites and email accounts, then release the information publicly for anyone to use. In some cases, depending on what your security settings are, anyone can access your information, including disgruntled coworkers, the media, or gangs in your community.

A new guide from the Office of Justice Programs (OJP) talks about how criminals might investigate you using your digital footprint, or those of your family, friends, and associates, and use posted information against you. "Understanding Digital Footprints: Steps to Protect Personal Information" talks about tactics criminals use, how they find your information, and what you can do to protect it.

Limiting your digital footprint and protecting your information is a process, not a one-time task. The OJP guide offers some quick fixes, like adjusting social media security settings, and more time-consuming tasks, such as removing personal data from online "data broker" sites, like PiPl. Taking the time to work on this issue may save you a great deal of hassle later.

(Source: OJP)

How 9/11 Changed Public Safety Communications

Major disasters are often the catalyst for changes in established practices and systems. Being suddenly faced with a mammoth undertaking has a way of shaking systems loose and making way for new, often better or faster systems. September 11th did this for public safety communications.

The police-fire interoperability problems in New York City was a critical flaw talked about for years, but lack of interoperability affects much more than just police-fire. At times, people in buildings cannot communicate with their counterparts outside the building, agencies on shore cannot coordinate with the Coast Guard or others on the water, and in many cases lives depend on these connections.

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

FirstNet.gov produced a video blog series looking at how public safety communications have changed since 9/11 and what new technology will bring in the future. The short videos feature first responders sharing their experiences of 9/11 communications, the limitations of the 2001 technology, and how far we've come in the past 15 years.

FirstNet was signed into law in 2012 to create public safety's first high-speed, nationwide wireless broadband dedicated network. It is intended to become the interoperable platform first responders need to fix the problems listed above.

(Source: FirstNet.gov)

Wireless Alerts, Surveillance Cameras Aid Manhunt

After the FBI identified a person of interest in the New York/New Jersey bombings, they put into effect some technology that up to that point had only been used in weather advisories or alerts for abducted children. For possibly the first time, the Wireless Emergency Alerts system pushed an electronic wanted "poster" out to cellphones in the greater New York City area, bringing millions of people in on the manhunt for the alleged bomber.

The ability to geographically target a specific area makes this feature a very valuable tool for authorities trying to get critical messages out, but one that could make the public ignore them if used too much. The messages are also limited to 90 characters. If used during some disasters, such as a dirty bomb attack, crafting a clear message that will not incite fear may be a challenge.

Authorities also used surveillance video, as they did during the Boston Marathon Bombing, to identify people in the areas of the bombings and track their movement. The many security and traffic cameras in use give authorities the ability to confirm that someone may – or may not – be involved in an incident, and they provide many chances to get clear photos of suspects. Downsides include privacy concerns and the sheer amount of video to sift through, but coupled with facial recognition, this technology shortens the time to identification and capture.

(Source: New York Times)

Fire Prevention Week: Don't Wait - Check the Date

This year, Fire Prevention Week hits October 9-15th and the theme is "Don't Wait – Check the Date! Replace Smoke Alarms Every 10 Years."

This is the third year in a row focusing on smoke alarms. The National Fire Protection Association (NFPA) survey data shows there are still a lot of misconceptions about smoke alarms nationwide, and this puts people at more risk for home fires. Many people don't know how old their smoke alarms are, and those who do may not know how often they should be replaced.

To help departments fill that knowledge gap on smoke alarms, both NFPA and the U.S. Fire Administration offer some community outreach tools, including infographic posters, Facebook and Twitter dynamic GIFs, handouts and trifolds, and a short video featuring Dan Doofus, who desperately needs help with his smoke alarm.

(Source: NFPA)

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**.