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

The InfoGram

Volume 18 — Issue 5 | February 1, 2018

Backing up deaths can be prevented

Four fire service personnel have died in the past two years from incidents involving emergency apparatus backing up. These deaths are totally preventable with proper training, use of spotters and other safety practices.

ResponderSafety.com released the "Backing Up Best Practices" guide and video to address this problem. These resources help departments implement life-saving safety practices and aid in standard operating procedure (SOP) development. ResponderSafety.com recommends backing up SOPs should include:

- Guidance to only back up when absolutely necessary.
- A defined backing up procedure which includes a spotter, defined roles of driver and spotter, and high-visibility PPE requirements.
- Mandatory visual inspection of the apparatus and surrounding area.
- Defined situations requiring immediate vehicle stoppage.
- Use of lighting and visibility aids at night.
- Consider retrofitting back up cameras on apparatus as a backing aid, not as a replacement of the spotter.

The single most effective thing a department can promote is also the simplest: **avoid backing up**. It may seem silly and inconvenient, but a small amount of inconvenience can save someone's life.

(Source: ResponderSafety.com)

Protecting your data: privacy and safety online

Identity theft is often a crime of opportunity. If your information is available online, or if your data was breached, you are more likely to be a victim. While we have little control over data breaches, we can control how much information we put online. A recent McAfee study shows just how bad we are at data security:

- Only 59 percent of those polled immediately change default passwords.
- Only 37 percent use credit monitoring services. Fewer monitor a child's credit.
- Only 66 percent limit who can access their home networks.
- 33 percent of parents don't know the risks well enough to explain the dangers to their children.
- 52 percent aren't sure how to secure connected devices or apps.

There are many things you can do to help keep your data secure and you don't need to be an information security guru to do it. The United States Computer Emergency Readiness Team (US-CERT) has resources available to walk you through the steps to safeguarding your data, protect your privacy, recognize and avoid social engineering and phishing attacks, and how to prevent and respond to identity theft.

If you believe you are the victim of an internet-related cyber crime, you can report

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.

it to the Internet Crime Complaint Center (IC3). The IC3 investigates a range of activity including hacking, identity theft, and types of corporate espionage crimes.

(Source: US-CERT)

Preliminary report on the Mandalay Bay mass shooting

The Las Vegas Metropolitan Police Department (LVMPD) released its preliminary report on the October 2017 mass shooting at the Mandalay Bay (PDF, 4.5 MB), which killed 58 and wounded over 700.

LVMPD details the shooter's actions and preparations leading up to the shooting. It also outlines his personality and mannerisms through the eyes of people he knew, and documents his Internet search history and how it changed over time. His motive for the shooting remains the topic of speculation.

Many things in this report can be used for planning and training for future incidents. The LVMPD goes into great detail about the shooter's surveillance methods during the shooting. It also documents his pre-attack surveillance, information gathering, possible target selection and acquisition of supplies.

Individually, these actions may not be questionable. However, all are parts of the terrorist attack planning cycle. Officials did not name this as an act of terrorism, but incidents such as these often share similar planning methodology and indicators.

We should stress this is a preliminary report; the investigation is not yet complete and the information contained in this report will likely change or be updated in the final report, to be released when the investigation is complete.

(Source: LVMPD)

National EMS Scope of Practice Model released for public comment

The National Association of State EMS Officials (NASEMSO) requests public comment on the recently released draft "National EMS Scope of Practice Model." The draft was released after a two-year collaboration with the National Highway Traffic Safety Administration.

The draft includes descriptions of the four provider levels and the proposed process for rapidly updating the Practice Model if situations arise that require it.

The rapid update procedure was tested last year to address three timely, life-saving changes. As of November 1, 2017, those with Emergency Medical Responder and Emergency Medical Technician licenses are able to:

- Administer narcotic antagonists.
- Apply tourniquets.
- Use wound packing.

Comments on draft provider level descriptions and the proposed process for rapid changes to the Practice Model must be submitted online by February 10, 2018.

(Source: EMS.gov)

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.**

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.