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

The InfoGram

Volume 19 — Issue 26 | July 25, 2019

FBI quick reference guide on active shooter pre-attack behaviors

The FBI Behavioral Analysis Unit released the Quick Reference Guide (PDF, 506 KB) for the "Study of the Pre-Attack Behaviors of Active Shooters in the United States between 2000 and 2013."

The two-page guide lists demographics, known stressors, methods of planning and preparation, mental health statistics and indicators, social connections, firearms acquisition, and several sections relating to concerning behaviors and known grievances. Of those that had an identifiable grievance, 44 percent experienced a "triggering" event related to that grievance.

Despite shooters displaying behavioral changes that were noticed by friends, family or others close to them, over 50 percent of those concerned about the individual did not report their concern to anyone. Educating people on how to recognize such indicators, where to report them and encouraging people to do so may help prevent future attacks.

The FBI stresses there is not a single "profile" of an active shooter and there is no single warning sign, checklist or algorithm for identifying a potential active shooter. However, it is still possible to prevent such attacks through effective threat assessment and management.

The full FBI study goes into greater detail including definitions, analyses and conclusions related to specific sections of data, and more.

(Source: FBI)

New NTAS bulletin focus on homegrown threats

The Department of Homeland Security (DHS) issued a new National Terrorism Advisory System (NTAS) Bulletin last week. The new bulletin again focuses on homegrown violent extremists, updating the information released in the expired January 2019 NTAS bulletin.

This bulletin aims to increase the public's knowledge and understanding of the threats facing the United States, including attacks using vehicle ramming, small arms, straight-edged blade and homemade explosives. The bulletin also discusses homegrown terrorist use of technology, unmanned aerials systems and the use of social media to communicate.

These tactics have been used in Europe over the past few years with varied success. The updated bulletin lists who to contact to report suspicious activity, what to do to be prepared and how to stay informed.

The NTAS system can have three types of advisories: a general bulletin, an elevated alert and an imminent alert. Since its revision in 2015, only bulletins have been issued.

(Source: DHS)

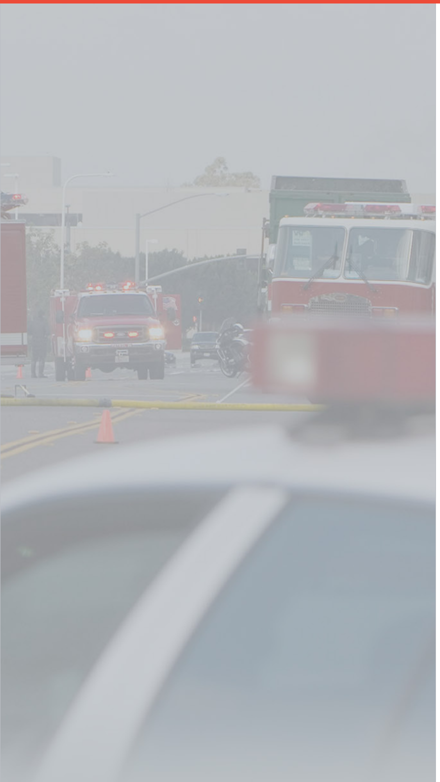
Highlights

U.S. Fire Administration

The U.S. Fire Administration operates 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.

Subscribe here



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.

Disclaimer of Endorsement:
The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.

Millennials might just be what the fire service needs

Millennials, those born approximately between 1980 and 2000, have gotten a lot of press the past few years. Not much of it is very flattering. This generation is quite different in lifestyle, social interactions, values and expectations. For a field as set in tradition and resistant to change as the fire service, transitioning this generation into its ranks may be a challenge. But it doesn’t have to be.

Regardless of all that negative press and the preconceived notions you may hold, consider the following: the Millennial generation is bigger than the Baby Boom generation by about 15 million people; they take health and physical fitness seriously; they grew up with new and evolving technology and are “digital natives;” and they embrace diversity of all kinds and are a very diverse generation.

In this time when the fire service is struggling to integrate technology, embrace diversity and, in some cases, desperately needs to fill in dwindling ranks, the traits listed above seem to fit the bill. Now, how do you successfully recruit them?

Though this article by Rackspace is about spending habits, it offers sound marketing ideas departments can use to engage Millennials as volunteers or employees. Here are some key takeaways:

- Be where they are. Without an active social media presence, you are missing them entirely.
- Provide experiences and seek authentic engagement. Your department or agency’s brand must have a human face and a conversational voice.
- Video is a critical medium. Millennials spend 48 percent more time watching online videos than other age groups.
- Speak to their values. Social causes are important to them.

FireRescue1 offers an in-depth look at Millennials’ implication to the fire service. For more information on recruting Millennial volunteers, see this article from the National Volunteer Fire Council.

(Source: FireRescue1)

IPSA 2019 Natural and Manmade Disaster Recovery Symposium

Natural and man-made disasters are unavoidable and will always be a part of our world. Public safety officials are taxed with additional responsibility when disaster strikes, and they perform duties beyond their standard scope of practice. There are best practices, lessons learned and resources that exist to aid short-term and long-term disaster recovery.

The International Public Safety Association (IPSA) is hosting an educational training symposium September 18-19, 2019, in the Washington, DC, metro area. This event is for all first responders (law enforcement, corrections personnel, firefighters, EMS, 911 dispatchers), allied emergency responders, government officials and communities of practice.

Attendees will walk away with several educational resources, tips and ideas they can apply in their agency and jurisdiction. For details on the agenda, session topics, and to register, see the IPSA website.

(Source: IPSA)

Cyber Threats

Ransomware attacks rampant, paying still not a good option

A flurry of ransomware attacks reported this week affected entities in Georgia, New York, Tennessee and Florida. File-encrypting malware has grown rampant lately, with the likes of Ryuk, Sodinokibi, or Dharma/Phobos targeting organizations in both the public and private sector. The actors behind these threats do not discriminate between targets but statistics from a ransomware incident response company show **public sector victims pay ten times more than private companies**.

(Source: BleepingComputer)

Insider attacks more difficult to detect, prevent than external attacks

A recent survey conducted of more than 320 IT security experts found that **15 percent of people said they would delete files or change passwords upon exiting a company**.

(Source: HelpNetSecurity)

Webinar: Holistic Approach to Mitigating Insider Threat

On July 29, the Cybersecurity and Infrastructure Security Agency will host a webinar on a **holistic approach to mitigate insider threat**. Experts on the webinar will discuss how to prevent, mitigate, and respond to cybersecurity insider threats in all types of organizations.

- Date/Time: July 29, 2019 @ 2:00-3:00 p.m. ET
- Webinar Link: https://share.dhs.gov/cisawebinars; Dial-In: 1-800-909-4578

(Source: CISA)

Why 72 percent of people still recycle passwords

Despite the risk and reality of cybersecurity breaches in the enterprise, the majority (72 percent) of people said they still recycle passwords.

Reusing old passwords can easily result in a type of cybersecurity breach called credential stuffing, the report said, which allows hackers to take information from a previous breach to gain access to other accounts.

The majority of respondents who have been hacked already (89 percent) said they changed their passwords habits upon finding out the attack happened, the report added.

(Source: TechRepublic)

Are you still running Windows 7? Microsoft ends support in 2020

Despite the awareness that **in six months Microsoft will officially end its support for its nearly 10-year-old operating system Windows 7**, 18 percent of large enterprises have not yet migrated to Windows 10, according to new research. At the start of 2019, researchers found that 43 percent of companies were still running Windows 7. Of those, 17 percent didn't even know about the end of support.

(Source: InfoSecurity)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information

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