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

The InfoGram

Volume 19 — Issue 14 | May 2, 2019

Hazardous Materials Roundtable Meeting Report

After an 8-year lapse in the International Association of Fire Chiefs (IAFC) roundtable of hazardous materials (hazmat) response, they reconvened the roundtable process this year with the U.S. Fire Administration (USFA) and the Pipeline and Hazardous Materials Safety Administration (PHMSA). The meeting report has just been released.

Hazmat response spans several different fields within the emergency services, and often incorporates private sector partners. Because of this and other factors, they are complex incidents requiring proper prior planning and well-executed response, management, mitigation and recovery.

During the roundtable, several themes emerged:

- Information sharing efforts have improved over the last decade; however, the hazmat preparedness community lacks a system to gather, analyze, package and distribute critical information in a timely manner.
- There's a continuing need for improved community hazard awareness and more education for the public on their expected role and responsibilities.
- It's still challenging to provide effective training content, availability and delivery.
- Good leadership at the local and state level is critical to develop and maintain effective response.

Participants strongly recommended roundtable meetings continue on an annual basis.

(Source: USFA)

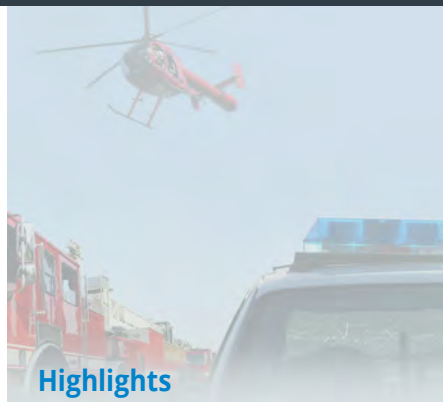
National Significant Wildland Fire Potential Outlook

According to the National Interagency Fire Center (NIFC) in Boise, Idaho, the Pacific Northwest and Hawaii have an above normal likelihood of significant wildfires through at least August. California and the Southwest also may see above normal wildfires.

The NIFC maintians predictive maps to inform fire management decision makers of current and expected wildland fire threat. It develops two maps: a monthly map for the current and each of the next three months; and 7-day significant fire potential map, only produced during fire season. The 7-day maps are available as static maps or as an interactive viewer.

In addition to the maps, the NIFC produces a report on expected wildland fire activity over a 4-month period. This report discusses moisture and drought conditions across the country, weather and climate outlooks, and breaks down forecasted wildland fire potential by geographic area.

(Source: NIFC)



Highlights

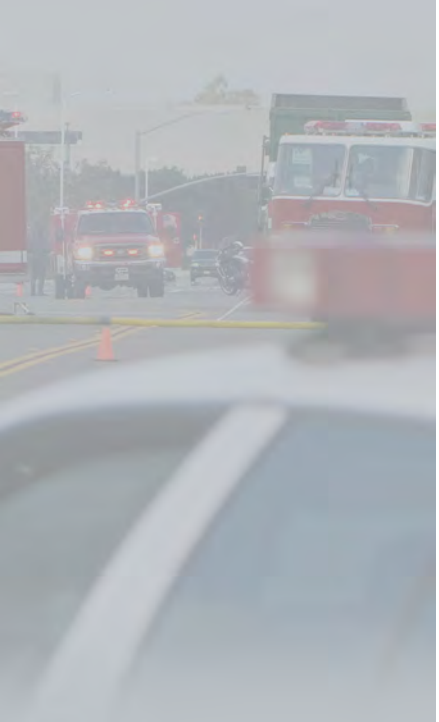
Cyber Threats

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



Security of Soft Targets and Crowded Places - Resource Guide

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released "Security of Soft Targets and Crowded Places - Resource Guide" (PDF, 6 MB) last week.

This guide catalogs resources such as training, tools, videos and websites to assist individuals and both the public and private sectors to secure soft targets. Terrorists and other extremists continue to target these locations for several reasons: they require minimal planning and simple tactics; potential targets are plentiful; and often there is easy access and limited security onsite.

Resources for first responders, businesses, government entities and citizens are broken down into these categories:

- Understand the Basics
- Identify Suspicious Behavior
- Protect, Screen, and Allow Access to Facilities
- Protect Against Unmanned Aircraft Systems
- Prepare for and Respond to Active Assailants
- Prevent and Respond to Bombings

This is an invaluable resource for anyone working to minimize the threat to public places and large gatherings.

(Source: CISA)

InfoGram to feature cybersecurity information for first responders

The Emergency Services Sector and related fields are experiencing cyberattacks as a growing threat. The Sector is increasingly dependent on systems and tools requiring networking capabilities and electronic data storage. Local jurisdictions should expect to see increased incidents of cyberattack going forward.

To address this growing threat, The InfoGram will have a new third page starting this week featuring cybersecurity threat and vulnerability information. We will also feature information to help you keep your networks, data and personnel safe from cyberattacks.

Resilience against cybercrime is new territory for many locales and is just one more thing competing for time and resources against the natural and man-made disasters already on the table. However, your systems and data are vulnerable. Proper firewalls, virus protection, upgrades, regular data backups and effective training is a small price to pay to keep a potential $400,000 ransom at bay.

Though we will focus on threats that are affecting, or could affect, the Emergency Services Sector, some of the information will be equally applicable to related fields and for cybersecurity at home as well.

In addition to the threats being highlighted weekly, there is a list of cybersecurity resources on the left sidebar. These supply you and your organization with training and resources, and also list agencies you should report ransomware attacks or other cyberattacks to.

(Source: EMR-ISAC)

Cyber Threats

Emotet hijacks email conversation threads to insert links to malware

The Emotet malware gang is now using a tactic that has been previously used by nation-state hackers. The group has been spotted this week **reviving old email conversation threads and injecting links to malicious files**.

Users involved in the previous email exchanges would receive an email spoofed to appear from one of their previous correspondents, but actually coming from Emotet servers. The email conversation thread would be left intact, but the Emotet gang would insert an URL at the top of the email that would link to an Emotet-infected file, or attach a malicious document to the existing email thread.

(Source: zdnet)

LockerGoga: Ransomware Targeting Critical Infrastructure

FortiGuard Labs Threat Analysis Report: since the discovery of Stuxnet, **more and more cyberattacks are being discovered targeting critical infrastructures**. While some attacks are sophisticated and some are not, both can cause significant damage with far-reaching impact.

In the early age of ransomware, these attacks were not primarily used to target critical infrastructure. But recently, the FortiGuard Labs threat research teams have seen an increasing trend of ransomware attacks targeting critical infrastructures using attacks such as WannaCry, NotPetya, SamSam and now LockerGoga. This says a lot about the future of ransomware.

(Source: Fortinet)

IT pros fear employee error, not hackers, will cause the most breaches

Security analytics firm Gurucul has released a new report on the growing insider threat to organizations. The survey conducted among over 650 Information Technology (IT) professionals from various countries indicates that **nearly three out of four organizations are vulnerable to insider threats**.

Companies consider the biggest insider threats to be user error (39 percent), malicious insiders (35 percent) and account compromise (26 percent). A particularly worrisome finding is that only around one-third (34 percent) of organizations believe they can detect threats in real time. According to the report, manufacturing firms are most at risk, followed by organizations in the health care sector.

(Source: OODA Loop)

Medical Advisory: Tasy Electronic Medical Record (EMR) exploitation

Successful exploitation of this vulnerability could impact or compromise patient confidentiality and system integrity. Philips' analysis shows these issues, if fully exploited, may **allow attackers of low skill in the customer site** or on a VPN to provide unexpected input into the application, execute arbitrary code, alter the intended control flow of the system, and access sensitive information.

(Source: US-CERT)

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