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

The InfoGram

Volume 20 — Issue 38 | September 17, 2020

NFFF produces new LODD course for incident commanders

The National Fallen Firefighter Foundation (NFFF) released a new course in July, one you will hopefully never need.

When an LODD Occurs: Incident Commanders Speak is a 1-hour training to help prepare incident commanders (ICs) for the unique challenges that occur in the aftermath of a firefighter line-of-duty death (LODD).

The course supports the IC to IC Network, providing support to incident commanders who have experienced a LODD on their watch. The NFFF has found ICs face a series of emotional, personal, political, social, legal and relationship effects after a LODD. The IC to IC Network connects ICs who have faced these tragedies.

The program will:

- Educate ICs about what they might face if a LODD occurs during a response where they are in command so they can be better prepared.
- Be a resource for ICs of scenes where a LODD has occurred, functioning as a source of support and guidance for how to navigate the aftermath that will forever change the IC and the department.

The NFFF encourages ICs to take this course and look into the IC to IC Network. It will be a source of support for ICs during a time or crisis.

(Source: NFFF)

Evaluating your department's COVID-19 response

While many locations are still waiting for a much-needed lull in pandemic response, it's not a bad idea to begin evaluating your initial response in order to identify what worked and what needs improvement going forward.

Occupational Health and Safety magazine recently ran an article suggesting things to consider when performing an evaluation of your COVID-19 response.

Some guiding questions and suggestions for a good evaluation:

- Did the organization take a proactive or reactive approach?
- Did you have problems finding needed supplies (PPE, medical equipment, etc.)? Are you prepared with back-up suppliers if it happens again?
- Were your existing plans and procedures up-to-date? Did they work? If the answer to either of these questions is no, have they been updated?
- How quickly did leaders make decisions? Were they communicated quickly to the organization? How can this be improved?
- Write notes on problems or concerns when they happen so you don't forget.
- Others will look at the decisions you made. While this may be uncomfortable, you can prepare by reviewing your decision-making process beforehand.

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

Evaluations like this can help you and your organization better meet the next challenge by identifying and addressing problems now.

(Source: Occupational Health and Safety)

How near-misses affect personal preparedness

Many factors affect how people prepare for and evacuate before a disaster: prior experience, gauging what friends and neighbors are doing, official messaging, media reporting, etc.

One variable is previous near-misses. Researchers define a near-miss as an event in which a person has a non-trivial expectation of experiencing a disaster but, by chance, does not. Recent research shows a relationship between near-misses and preparedness, but it seems to depend on the nature of the near-miss event.

The new research suggests is there are two different types of near-misses: resilient and vulnerable. People tend to view near-misses as either "our system is strong" or "we dodged a bullet." People who have a vulnerable near-miss viewpoint are more likely to prepare for future disasters.

Visit the Natural Hazards Center to see the brief on this new research, which looked at and expands on similar studies from the 1990s.

(Source: NHC)

Countering false information on social media in disasters

The internet is often a hotbed of false and inaccurate information. Agencies and organizations responsible for keeping the public safe have their work cut out for them when battling false information and, unfortunately, the problem has gotten more complex as new technologies, social media platforms and agendas emerge.

The Department of Homeland Security's Social Media Working Group for Emergency Services and Disaster Management white paper "Countering False Information on Social Media in Disasters and Emergencies" can help agencies with this issue.

The white paper examines what motivates people to share bad or false information and discusses underlying issues causing false information. It looks at several real-world case studies to provide agencies several best practices to counter misinformation, rumors and false information.

False social media content is most often caused by four issues:

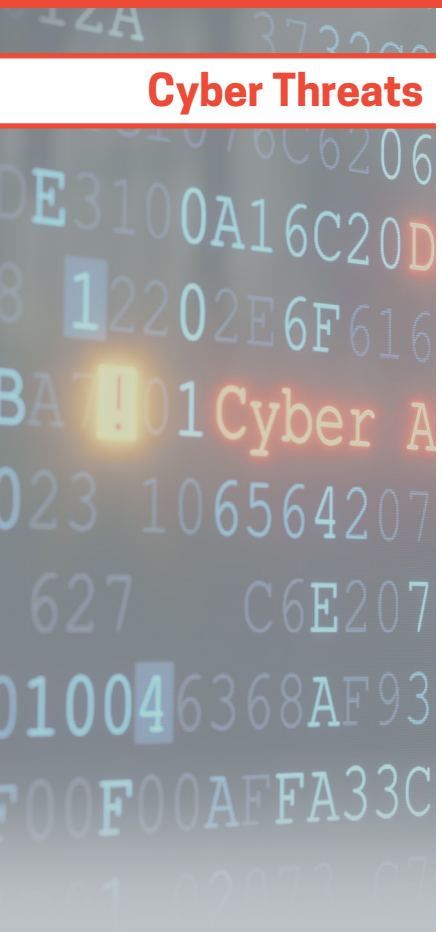
- Incorrect Information (can be intentional or unintentional).
- Insufficient Information.
- Opportunistic Disinformation.
- Outdated Information.

The white paper examines each of these issues in depth. It explores key best practices categorized by people, processes and technology such as partnerships, software considerations and advanced preparation.

Members of the working group are subject-matter experts from federal, tribal, territorial, state and local responders. They establish and collect best practices and solutions to be implemented by public safety officials and first responders.

(Source: DHS)

Cyber Threats



How cybercriminals attack SLTT organizations

Cybercriminals continue to target state, local, tribal and territorial (SLTT) government organizations at an alarming rate. Attackers often target SLTT organizations because they know their security teams need to run complex networks, as well as deal with numerous third-party systems and services.

Many SLTT cybersecurity teams are also struggling with reduced security budgets and a well-documented shortage of skilled cybersecurity and networking professionals to fill open positions. COVID-19, and the subsequent increase in remote working by government employees and online accessibility requests for government resources by citizens, has only added to their security challenges.

To help SLTT organizations protect themselves against these common types of cyber-attacks, the Center of Internet Security (CIS) is partnering through the MS-ISAC and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) with the U.S. Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA) and Akamai to offer its new Malicious Domain Blocking and Reporting (MDBR) service at no cost to SLTT government members of the MS- and EI-ISACs. The service allows SLTT security teams to quickly add an additional layer of cybersecurity protection against their systems connecting to malicious web domains and to enhance their existing network defenses.

(Source: Center for Internet Security)

US court documents published in ransomware attack

Cybercriminals who launched a ransomware attack on the Fourth Judicial District Court of Louisiana published what they claim are stolen court documents online.

Alleged proof of the attack was published on the dark web this week. Those claiming responsibility for the crime have uploaded what appear to be court documents exfiltrated in the incident.

Among the allegedly swiped documents are responsive verdicts for a second-degree kidnapping, an armed robbery and a case of aggravated rape. Other documents appear to relate to excuses given by jurors and a meeting of judges.

The website of the Fourth Judicial District Court of Louisiana is currently offline. Details of how big a ransom the attackers are demanding have not been revealed.

(Source: InfoSecurity Magazine)

ProLock ransomware - everything you need to know

Since the start of the year, a new ransomware gang named ProLock has made a name for itself by hacking into large companies and government networks, encrypting files and demanding huge ransom payments.

ProLock is the latest ransomware gang that has adopted the "big-game hunting" approach to its operations. Big-game hunting refers to going after larger targets in order to extract big payments from victims who can afford it.

System administrators who manage these larger networks are most likely to see attacks from this particular group.

(Source: zdnet)

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.