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

The InfoGram

Volume 17 – Issue 11 *March 16, 2017*

Highlights:

Disclaimer of Endorsement:
The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.

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.**

Cyber Best Practices for Emergency Services

Cybersecurity concerns continue to be an issue for the Emergency Services Sector. The Department of Homeland Security (DHS) recognizes that departments and agencies have different levels of skills and resources available to address the issues, and many lack the facts. DHS has addressed these issues by publishing "Emergency Services Sector Cybersecurity Best Practices" (PDF, 841 Kb).

This 3-page guide lists quick, actionable, often easy things you can do to ensure your department is safe from ransomware and other cyberattacks, such as:

- Set devices to automatically sleep or shut down when not in use;
- Restrict personal use of agency devices;
- Change default passwords on all devices that come with one;
- Post pictures online understanding everyone may having access to them;
- Treat unsolicited emails or suspicious emails with caution;
- Turn off the settings for automatic downloads of attachments.

These fast, preventative measures can easily be turned into a departmental policy or Standard Operating Procedure (SOP), making safeguarding the organization everyone's job. Also, these measures should be incorporated into personal and family habits in order to secure financial information, family details, photos, and physical security.

(Source: DHS)

The Balance Between Building Security & Safety

September 11th changed the safety and security landscape in the United States and that trend has continued in part due to active shooters, lone wolf terrorist attacks, and the coordinated attacks seen primarily in Europe. Security remains at the top of the list for public buildings and it battles with other, more probable safety concerns.

In a 2009 Society for Fire Protection Engineers survey, 28 percent of Americans said security was the most important consideration for public buildings. Only 12 percent felt fire safety was most important even though fires are much more likely to occur. In other words, the public is still more than 2-to-1 in favor of increasing physical security over life safety measures in public buildings (PDF, 35.7 Kb).

Security managers can then be put in a difficult position of increasing building security at the expense of safety and even sometimes being expected to enact security measures in direct violation of fire and life safety codes.

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

It is vital code inspectors and fire marshals work with security managers to ensure security measures don't obstruct life safety. For example, limiting the number of entrances to serve as staff security checkpoints, but at the same time ensuring all egress options are available in the event of a fire. Both security and life safety are important, but they must strike the right balance and be in compliance with codes and standards.

(Source: SecurityMagazine.com)

Attack Overseas Concerning for Hospital Security

While many believe targeting medical facilities is abhorrent, even in war, they remain an attractive target for many terrorist groups. There were approximately 100 terrorist attacks against hospitals between 1981 and 2013. Attacks against hospitals and other medical facilities provide terrorists a high casualty rate, lots of media coverage, and invoke fear and horror among the populace.

Last week, four fighters linked to the Islamic State of Iraq and the Levant (ISIL) attacked a military hospital in Kabul, Afghanistan. They wore white lab coats and surgical masks and drove an ambulance. The siege lasted six hours and included AK-47s, knife attacks, a suicide bomber, and a car bomb. Fifty people were killed and 30 wounded, many of them civilians and medical staff.

It is important to note there is currently no credible, specific threat to hospitals in the United States; however, ISIL has encouraged its followers to attack hospitals in the West through English-language propaganda magazines.

It is concerning that the Kabul attack was so successful against a military facility in a region that regularly sees and prepares for violence. Such an attack against a civilian target in a less violent region would likely be worse. Security staff at these facilities should be looking at improving their security measures to include how they handle credentialing and staff admittance into the facility.

(Source: ICT)

Stop the Bleed Program and Webinar

It is possible for a heavily-bleeding victim to die from blood loss in less than 5 minutes. This is well outside the response time for many areas and in these circumstances bystanders may be the victim's best chance for survival. Ensuring those bystanders have the necessary skills and training is crucial to increasing survivability of victims.

The Department of Homeland Security (DHS) program "Stop the Bleed" is designed to teach the public how to manage a bleeding victim before help arrives. The DHS website links to online training, how to use a tourniquet, a video showing the difference in response between trained and untrained school personnel, and other resources and videos that can be used in targeted campaigns to train the workforce at educational facilities, churches, public venues, governmental facilities, and more.

The Emergency Medical Services for Children (EMSC) is offering a webinar on the Stop the Bleed program on March 29, 2017 from 3:00 p.m. to 4:00 p.m. Eastern. It is an introductory brief on the program, recommended for EMSC personnel. There is a limit to the number of callers so be sure to register early and try to have multiple people on one line to allow more participants access. The webinar will be recorded and posted on the EMSC site for those unable to call in.

(Source: DHS)

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**.