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

The InfoGram

Volume 19 — Issue 13 | April 25, 2019

Communications strategies for global catastrophic biological risks

A Global Catastrophic Biological Risks (GCBR) is a biological development that could adversely affect the human species as a whole or radically change the course of human civilization. These high-impact, low-frequency events are hard to predict, presenting a challenge for effective risk communication.

A Johns Hopkins Center for Health Security research project focuses on this issue, defining what constitutes a GCBR, looking at historical global-scale threats and then examining what it takes to get people with knowledge, influence and control of resources to understand the potential ramifications of a GCBR.

The team looked at modern events such as the anthrax attacks in 2001, Zika, Ebola, and the Cold War threat of nuclear winter to see the good and bad risk communication and how policymakers and the public responded. They list a number of recommendations for future GCBR communications, including some that can be leveraged at the local level:

- Continually update risk assessments and risk reduction strategies.
- Enlist subject matter experts as communicators.
- Identify and utilize stakeholders from non-health arenas.
- Advocate both individual and social obligation when discussing the threat.

(Source: Johns Hopkins Center for Health Security)

Dark Web primer: how much are you worth to a cybercriminal?

The Healthcare Cybersecurity Coordination Center (HC3) recently produced an unclassified brief on the Dark Web. Though it focuses on protected health information (PHI), the brief is a very good primer on the Dark Web in general, how criminals buy and sell your personal information, how much you are worth on the Dark Web and how to better protect your information.

The internet is divided into layers. Most of us are familiar with the Surface Web consisting of public-facing sites we use every day: search engines, commerce sites and other business or government websites. The next layer, the Deep Web, can be accessed by typing in the direct web link, and may require you to log in. LinkedIn profiles, anything you have a subscription for and your bank account are examples.

The Dark Web is encrypted. It is intentionally hidden from standard web browsers and can only be accessed through special software. This is where black market and illegal activities such as drug dealing and child pornography happen.

Stolen personal information is traded and bought on the Dark Web. HC3 states a person's finance details and proof of identity can go for as little as $1,170. This is a bargain when you consider the return on investment for the criminal, as it gives them your digital life for the taking. Children's data for sale is also trending.

Individuals should not assume any information stored electronically is fully protected from data breaches or cyberattack. Monitor all financial, medical and personal information regularly and address discrepancies immediately. Consider using a

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.

fraud monitoring service, as it will do much of the work for you.

(Source: HC3)

PrepTalks and webinar on supply chain resilience

The Federal Emergency Management Agency (FEMA) announced new resources on supply chain management during disasters.

"Aligning Public and Private Supply Chains for Disaster Response" demonstrates how the private sector has more capacity to respond than the public sector, explains the role of emergency managers in supporting private sector supply chain restoration and shows how analysis helps strategic and tactical preparedness and operational collaboration during a crisis.

"Private Sector Resilience: It Is All In the Supply Chain" explains the modes of failure in supply chain networks and explores new ways to think about disruptions. The presenter also showcases a General Motors case study on the complexities of supply chain management.

In addition, FEMA's "Supply Chain Resilience Guide" provides recommendations and best practices to emergency managers on analyzing local supply chains and working with the private sector to enhance supply chain resilience.

The guide also identifies how emergency managers can use information from the supply chain resilience process to support restoration of supply chains and inform development or refinement of logistics plans or annexes, following the process described in FEMA's "Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans."

FEMA will host several webinars about this guide in the coming months. The next PrepTalks Symposium will be held on April 23, 2019, in Santa Rosa, California. A full schedule of speakers and topics is available on the website. Register now to attend!

(Source: FEMA)

Exercise to test 7.7 earthquake scenario near Memphis, Tennessee

Next month, FEMA is conducting the exercise Shaken Fury 2019 to evaluate and improve response to a 7.7 magnitude earthquake scenario along the New Madrid Seismic Zone near Memphis, Tennessee. The scenario affects six states.

The exercise will evaluate and improve whole community response to a no-notice event. It will test the coordinated response of federal, state and local governments; private sector partners; nongovernmental organizations; and critical infrastructures and utilities. Complex exercises such as these help identify gaps in response and recovery and improve them, making communities safer.

Organizations from the area that may be interested in participating should review the Shaken Fury 2019 Fact Sheet and contact FEMA-Exercise@fema.dhs.gov for more information.

(Source: FEMA)

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.