



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

**INFOGRAM 11-10**

**March 18, 2010**

***NOTE:** This INFOGRAM will be distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures. For further information, contact the Emergency Management and Response- Information Sharing and Analysis Center (EMR-ISAC) at (301) 447-1325 or by e-mail at [emr-isac@dhs.gov](mailto:emr-isac@dhs.gov).*

### More about Social Engineering

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) occasionally receives information regarding instances within the Emergency Services Sector (ESS) of [social engineering](#) particularly by electronic mail (e-mail). Social engineering is a method of fraudulently gaining access privileges to an organization's sensitive information by querying personnel via e-mail and other communications media such as the telephone, chat rooms, bulletin boards, etc.

According to an article in [The Register](#), the human factor is always the weakest link of the security chain. This reality was substantiated in the tests conducted by security penetration specialists. In their process, test administrators cleverly crafted e-mail with a malicious link and sent it to a large number of experiment participants. What they discovered was that their approach worked in nearly 50 percent of the cases.

When reporting their results, the researchers presented the following most common social engineering schemes and the psychological tricks that made them successful:

- Creating a sense of urgency.
- Developing a bond with the victim.
- Presenting a situation that throws the victim off-guard.
- Embellishing the situation causing the victim to suspend his or her critical capabilities.

To eliminate the potential exploitation from this type of e-mail or other communications, ESS personnel should be thoroughly aware of social engineering methods to enhance recognition and avoid adversary collection techniques. Therefore, the EMR-ISAC offers the [socyberty.com](http://socyberty.com) web site for current trends and prevention techniques.

### Preparing for 9-1-1 Calls

In an [article](#) prepared by Bob Smith, Director of Strategic Development for the [Association of Public-Safety Communications Officials](#) (APCO), the author referred to a report that between January and June 2009, 613 airplanes were delayed on American airport tarmacs between three and eleven hours. Having seen similar reports, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) noted consequences for the 9-1-1 call centers (i.e. Public Safety Answering Points) with airports in their jurisdiction.

The EMR-ISAC learned in some of the 600+ occurrences, passengers with cellular telephones called 9-1-1 for assistance with onboard medical emergencies, but more often alleged they were kidnapped or being held hostage. These cell calls from delayed aircraft asserting some type of criminal activity (e.g., kidnapping) quickly became a new challenge for the public safety communications industry.

Bob Smith advises affected jurisdictions to “develop policies and procedures for an appropriate response” to these types of calls. He recommends legal counsel “to assess the level of liability exposure the communications center will experience based on their response,” and to acquire answers to the following questions:

- What agency will be notified when these calls are received?
- Will the 9-1-1 center initiate any type of actual response to the airport for these types of calls?
- What parameters must be included in a computer-aided dispatch system to process these calls?
- How will calls from the media, family members of passengers, and others be processed?

Although there may be more questions or concerns for consideration, the author suggested taking time now to develop plans and procedures to expeditiously and professionally process each call of this type. APCO has a [Standards and Best Practices](#) site as well as a [Standards Development Committee](#) that could be of some value in pursuing this matter.

## First Responders: An Integral Part in Homeland Vigilance

As demonstrated daily throughout the nation, America’s first responders (e.g., police, fire, emergency medical technicians and paramedics) perform mission-essential tasks for man-made incidents and natural disasters. Regardless of whether the scene involves a hazardous material spill, methamphetamine laboratory, improvised explosive device, etc., “emergency responders should be adequately trained to investigate and mitigate the circumstances. They must be armed with sufficient training to understand the implications of what he or she is seeing,” according to a recent [takresponse.com](#) article, and “to recognize behaviors that should raise suspicions.”

Believing that Emergency Services Sector personnel are an integral part of homeland vigilance who must also keep well-informed and constantly aware of their situation, the [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) extracted the following general chemical, biological, radiological, and explosive indicators from [Homeland1 News](#) to enhance awareness:

- Theft of large quantities of baby formula or an unexplained shortage in the geographic area. (The formula can be used to grow certain specific lethal cultures.)
- Break-in or tampering with equipment at water treatment facilities, food processing plants, or warehouses.
- Theft or solicitation of live agents, toxins, or diseases from medical supply companies, or testing and experimentation facilities.
- Multiple cases of unexplained human or animal deaths.
- Thefts of agricultural sprayers, crop-dusting aircraft, foggers, river craft, or other dispensing systems.
- Suspicious inquiries regarding local chemical/biological/nuclear sales, storage, or transportation points and facilities.
- Inappropriate inquiries regarding heating and ventilation systems for buildings or facilities by persons not associated with service agencies.

More information regarding what to watch for in the performance of emergency services can be seen in the [brochure](#) (PDF, 299 KB) published by the New Jersey Office of Homeland Security and Preparedness.

## Web Site for Rail-Carried HazMat

The [Emergency Management and Response—Information Sharing and Analysis Center](#) (EMR-ISAC) received notification from the [Homeland Security Newswire](#) (HSNW) that railroad operator [CSX](#) now provides first responders and the [Chemical Transportation Emergency Center](#) (CHEMTREC) access to secure web-based information, which allows CHEMTREC to find a train number, tank car number, and identify what is being transported in those cars.

With this new capability, if a rail-carrier CSX train derails, emergency responders will have instant, real-time access to railroad manifests to learn whether the cars were hauling hazardous material (HazMat). The HSNW publication acknowledged that the technology already exists, with CSX providing real-time tracking of its hazardous cargo transports to CHEMTREC, which was designed to assist first responders with incidents involving HazMat and other dangerous products.

“It’s a web-enabled system that’s highly secure, that allows CHEMTREC to find a train number, tank car number, and identify what’s in those cars,” CHEMTREC director Randy Speight said. “It allows real-time access in seconds on the web.”

The EMR-ISAC confirmed that a [web site](#) is available for the use of the emergency services. Additionally, the CHEMTREC 24-hour HazMat Communications Center can be contacted at 1-800-262-8200.

## **DISCLAIMER OF ENDORSEMENT**

The U.S. Fire Administration/EMR-ISAC does not endorse the organizations sponsoring linked web sites, and does not endorse the views they express or the products/services they offer.

## **FAIR USE NOTICE**

This INFOGRAM may contain copyrighted material that was not specifically authorized by the copyright owner. EMR-ISAC personnel believe 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.

## **REPORTING NOTICE**

The National Infrastructure Coordinating Center (NICC) within the Department of Homeland Security (DHS) Office of Infrastructure Protection is the central point for notifications regarding infrastructure threats, disruptions, intrusions, and suspicious activities. Emergency Services Sector personnel are requested to report any incidents or attacks involving their infrastructures using at least the first and second points of contact seen below:

- 1) NICC - Voice: 202-282-9201, Fax: 703-487-3570, E-Mail: [nicc@dhs.gov](mailto:nicc@dhs.gov)
- 2) Your local FBI office - Web: [www.fbi.gov/contact/fo/fo.htm](http://www.fbi.gov/contact/fo/fo.htm)
- 3) EMR-ISAC - Voice: 301-447-1325, E-Mail: [emr-isac@dhs.gov](mailto:emr-isac@dhs.gov), fax: 301-447- 1034, Web: [www.usfa.dhs.gov/emr-isac](http://www.usfa.dhs.gov/emr-isac), Mail: E-108, 16825 South Seton Avenue, Emmitsburg, MD 21727